

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

The seal of the University of San Carlos of Guatemala is a circular emblem. It features a central figure, likely a saint or historical figure, seated and holding a book. The figure is surrounded by various symbols, including a crown, a lion, and architectural elements like columns and a building. The Latin text "ACADEMIA COACTEMALENSIS INTER CAETERAS CONSPICUA CAROLINA" is inscribed around the perimeter of the seal.

**EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y
LA VIDA PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA**

WILLIAM WELTER PORTILLO MENJIVAR

GUATEMALA, MAYO DE 2012

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

**EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y LA VIDA
PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA**



TESIS

Presentada a la Honorable Junta Directiva
de la
Facultad de Ciencias Jurídicas y Sociales
de la

Universidad de San Carlos de Guatemala

Por

WILLIAM WELTER PORTILLO MENJIVAR

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, mayo de 2012

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

DECANO: Lic. Bonerge Amilcar Mejía Orellana
VOCAL I: Lic. Avidán Ortiz Orellana
VOCAL II: Lic. Mario Ismael Aguilar Elizardi
VOCAL III: Lic. Luis Fernando López Díaz
VOCAL IV: Br. Modesto José Eduardo Salazar Dieguez
VOCAL V: Br. Pablo José Calderón Gálvez
SECRETARIO: Lic. Marco Vinicio Villatoro López

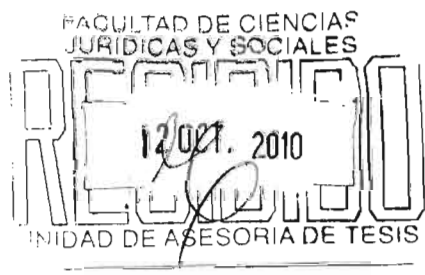
RAZÓN: “Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis”. (Artículo 43 del Normativo para la Elaboración de Tesis de la Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).



LICENCIADO MARIO ESTUARDO FALLA REYES
ABOGADO Y NOTARIO
12 Calle 1-25, Zona 10,
Edificio Géminis 10, Torre Norte, Oficina 610, Guatemala, Guatemala
Teléfono: 2335-3170

Guatemala, 7 de septiembre de 2010

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



Licenciado Castillo Lutín:

De conformidad con el nombramiento que me faculta como asesor, tengo el honor de informarle, que el trabajo de tesis, del bachiller **WILLIAM WELTER PORTILLO MENJIVAR**, nominado como **“EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y LA VIDA PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA”**.

En el referido trabajo de investigación que se presenta, en las sesiones de asesoría realizadas, se formularon al ponente, las modificaciones de forma y de fondo correspondientes, las cuales con su anuencia se incorporaron, enunciando los aspectos siguientes:

1. **Contenido científico y técnico de la tesis:** El sustentante le dio importancia al derecho a la privacidad, desde un punto de vista jurídico, social-administrativo, una investigación que aporta un valioso contenido en cuanto a la protección de los datos privados y reservados de las personas guatemaltecas.
2. **Metodología y técnicas utilizadas en la investigación:** es basado en el método deductivo e inductivo, analítico y sintético. En el presente trabajo de tesis, estuvo presente el elemento fundamental, la observación científica indirecta al apoyarse en obtener el mayor número de datos.
3. **Redacción:** El desarrollo del tema principal, se realizó en una secuencia ideal para que el lector le sea de fácil entendimiento.
4. **Contribución científica:** Importante aporte en el campo jurídico, al darle énfasis al derecho de la privacidad, que debe de gozar todo ciudadano guatemalteco.




LICENCIADO MARIO ESTUARDO FALLA REYES
ABOGADO Y NOTARIO
12 Calle 1-25, Zona 10,
Edificio Géminis 10, Torre Norte, Oficina 610, Guatemala, Guatemala
Teléfono: 2335-3170

5. **Conclusiones y recomendaciones:** La postura manejada del ponente en cuanto a proteger la vida privada del ser humano, en mi opinión contiene aspectos, importantes que deben ser tomados en cuenta, por los legisladores, estudiosos del derecho y la población en general.
6. **Bibliografía:** Se utilizó legislación internacional, autores internacionales, legislación nacional, relacionada al tema desarrollado.

Por lo expuesto anteriormente, emito el **DICTAMEN FAVORABLE**, en virtud que el trabajo de tesis de mérito, cumple con los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público. Para que sea discutido en el examen general de tesis.

Atentamente,



Lic. Mario Estuardo Falla Reyes
Abogado y Notario
Colegiado 8,648

Mario Estuardo Falla Reyes
Abogado y Notario

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.



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

Atentamente, pase al (a la) LICENCIADO (A) ALFONZO ROMEO CASTILLO CASTRO, para que proceda a revisar el trabajo de tesis del (de la) estudiante WILLIAM WELTER PORTILLO MENJIVAR, Intitulado: "EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y LA VIDA PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA".

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


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



cc. Unidad de Tesis
MTCL/sllh.



LICENCIADO ALFONZO ROMEO CASTILLO CASTRO
ABOGADO Y NOTARIO

7Av. Avenida 3-73, Zona 9, Edificio Torre SAT, 5°. Nivel, Ciudad de Guatemala, Secretaría General, Teléfono: 23297070

Guatemala, 05 de septiembre de 2011

Licenciado
Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala



Licenciado Castro Monroy:

En atención al nombramiento a mi persona para Revisar el trabajo de tesis del Perito Contador **WILLIAM WELTER PORTILLO MENJIVAR**, el cual se intitula **“EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y LA VIDA PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA”**, se informa que el mismo ha finalizado.

El contenido del trabajo es científico y de calidad, ya que el estudio y análisis del tema, desemboca en aportes útiles al derecho de privacidad de la persona contrastado con la libertad de información.

Sobre la metodología de la investigación, se realizó a través de la aplicación de métodos de tipo analítico y sintético, lo cual permitió que la redacción del trabajo sea adecuada, utilizando el ponente un lenguaje técnico acorde al tema desarrollado.

La contribución es valiosa en cuanto al derecho de privacidad de toda persona, considerado el espacio reservado en el cual se desenvuelve su vida, sin que la intromisión ajena tenga acceso a ella, frente al derecho al acceso a la información pública.

En tal sentido, considero que el trabajo de tesis de mérito, cumple con los requisitos reglamentarios del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que me permito emitir **OPINIÓN FAVORABLE**, para que sea discutido en el examen general de tesis.

Atentamente,

Lic. MSc. Alfonso Romeo Castillo Castro
Abogado y Notario
Colegiado 4895

Lic. Alfonso Romeo Castillo Castro
ABOGADO Y NOTARIO



DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.

Guatemala, dieciséis de abril del año dos mil doce.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de el estudiante WILLIAM WELTER PORTILLO MENJIVAR titulado EL CONFLICTO QUE EXISTE ENTRE LA LIBERTAD DE INFORMACIÓN Y LA VIDA PRIVADA DE LAS PERSONAS EN LA REPÚBLICA DE GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala.

LEGM/sllh



DEDICATORIA

- AL ALTÍSIMO:** Quien ha enderezado mi camino, y mis actos, este esfuerzo y éxito alcanzado a Jehová le pertenece.
- A MIS PADRES:** Manuel Antonio Portillo (QDP), y Antonia Menjivar Ruano, por la insistencia y apoyo para lograr alcanzar la meta de finalizar la carrera.
- A MI HERMANA:** Gilma Argentina, por su apoyo y motivación para culminar la carrera.
- A MI ESPOSA:** Refugio Raquel García Tejada, por su paciencia y por su ayuda en los momentos difíciles durante mi carrera.
- A MIS HIJOS:** José Welter y Ángel Josué, por su comprensión y cariño durante todo mi estudio.
- A MIS AMIGOS Y COMPAÑEROS:** Que me honran con su amistad y por los momentos felices que compartimos, mil gracias.
- A:** La Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales, lugar del saber y enseñanza, en los que hoy finalizo un peldaño más del éxito de mi vida personal.

ÍNDICE

	Pág.
Introducción.....	i

CAPÍTULO I

1. Derecho de acceso a la información.....	1
1.1. Concepto.....	3
1.2. Clasificación.....	5
1.2.1. Tipos de información.....	5
1.2.2. Conforme a doctrina.....	6
1.2.3. Conforme a Ley.....	8
1.3. Limitaciones.....	9
1.4. El impacto del uso de la Ley de Acceso a la Información Pública.....	13

CAPÍTULO II

2. Derecho de la informática.....	19
2.1. Información pública en la era informática.....	23
2.2. La informática y el derecho.....	26
2.3. La informática actual.....	27
2.4. Procesamiento de datos.....	29
2.5. Nuevos enfoques en la vida privada.....	30

CAPÍTULO III

3. Derecho de la privacidad.....	37
3.1. Concepto.....	41
3.2. Clases.....	43
3.3. Diferenciar privacidad e intimidad.....	49
3.4. Protección de los datos personales.....	53

3.5. El derecho de privacidad del individuo.....	Pág. 55
--	-------------------

CAPÍTULO IV

4. El Estado de Guatemala y el hábeas data.....	63
4.1. Definición.....	68
4.2. Datos personales.....	70
4.3. Amenazas tecnológicas.....	73
4.4. El derecho de las personas investigadas.....	77
4.5. Situación actual en la seguridad de información.....	79
 CONCLUSIONES.....	 87
RECOMENDACIONES.....	89
BIBLIOGRAFÍA.....	91

INTRODUCCIÓN

El presente trabajo de investigación, sin duda alguna el punto de partida es el respeto a la vida privada de las personas, tanto personal como familiar, por lo tanto constituye un valor fundamental del ser humano, razón suficiente que el derecho guatemalteco debiera tutelarlos y dictar medidas para evitar su violación. Se hace énfasis en que el ser humano, en la mayoría de los casos, se le ha vedado el derecho a defenderse, a declararse, a debatir aquello que se le imputa. Cada persona ha recibido de Dios el derecho a defender su personalidad, su libertad y su propiedad. Estos tres elementos son necesarios y requeridos para conservar la vida, son elementos que se complementan uno con el otro, pero estos derechos se han pervertido bajo la influencia de dos causas muy diferentes: el egoísmo carente de inteligencia y el falso idealismo.

En la actualidad, por los avances y a la vez por la ignorancia tecnológica en Guatemala, no existe una ley que proteja la personalidad de los individuos. Y la actual Ley de Acceso a la Información Pública, carece de normativa específica que proteja tal personalidad; sin sanción, sin el apoyo de una fuerza preponderante, es inevitable que en definitiva quede aquella fuerza en manos corruptas e inexpertas, la cual es manipulada a su conveniencia.

A raíz de la Conferencia de Derechos Humanos, realizada en Teherán quedó establecido el riesgo que implican los avances tecnológicos y científicos en lo que pudieran afectar a los derechos humanos. Es entonces, que la Asamblea General de la ONU recomienda a los Estados del mundo la realización de estudios con miras al dictado de normas que protegieran adecuadamente las libertades individuales especialmente las aplicaciones de las nuevas tecnologías que puedan afectar los derechos de las personas y los límites que deberían fijarse en torno a las mismas.

La justificación es que el derecho a la privacidad en Guatemala no está reconocido como tal en la constitución, protegiendo únicamente ciertas manifestaciones como los derechos a la inviolabilidad de domicilio, correspondencia, documentos y libros, lo que genera un vacío legal, generando a su vez violaciones a éste derecho.

La hipótesis es que al no estar regulado expresamente el derecho a la privacidad en el marco jurídico guatemalteco, deja la puerta abierta a la libre interpretación, por lo que se hace necesario, que el mismo se desarrolle a través de una ley ordinaria.

Es por ello que el objetivo principal es ubicar constitucionalmente el derecho fundamental a la privacidad, en el supuesto de que éste es inherente a la persona humana, inclusive anterior al propio Estado, todo esto para evitar que el Estado o los particulares lo invadan de una u otra forma.

Fue necesario el uso del método deductivo, inductivo, sintético, y de inferencia analógica tomando de base de estudio de varias Constituciones de distintos países de Latinoamérica y el continente europeo en donde la mayoría queda claramente protegido el derecho a la privacidad de las personas y sus datos personales.

Bajo esta perspectiva en el primer capítulo, se hace un estudio sobre el derecho de acceso a la información desde el punto de vista del impacto que se tiene y de la forma en que se está haciendo uso de la información pública en la República de Guatemala; en el segundo capítulo, se presenta un análisis sobre el derecho de la informática, cómo se trabaja el procesamiento de datos, cómo se desarrolla la tecnología actual y su injerencia dentro del marco legal; en el tercer capítulo, se hace un estudio del derecho a la privacidad desde su conceptualización, las distintas clases de información para llegar a determinar la diferencia que existe entre privacidad e intimidad y cómo esta última ha sido violentada y utilizada con fines de lucro; en el cuarto y último capítulo, se estudia el fenómeno del Estado y el Hábeas Data en relación a las amenazas tecnológicas, el derecho que tiene toda persona investigada y la situación actual que se enfrenta con la tecnología y los sistemas de información digital.

Finalmente en base a lo expuesto, de una manera sencilla, se considera necesario reformar la actual Ley de Acceso a la Información Pública, o en su defecto la necesidad de proteger mediante una ley específica, los datos personales y la vida privada de las personas guatemaltecas.

CAPÍTULO I

1. Derecho de acceso a la información

Según establece el Decreto 57-2008 Ley de Acceso a la Información Pública. El objeto de la Ley, Artículo uno numerales uno y dos es; “Garantizar a toda persona interesada, sin discriminación alguna, el derecho a solicitar y a tener acceso a la información pública en posesión de las autoridades y sujetos obligados por la presente ley;” y “Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos;”.

Este nuevo Decreto constituye una herramienta esencial para combatir la corrupción, hacer realidad el principio de transparencia en la gestión pública y mejorar la calidad de la democracia, signada por una cultura de secretismo y por organismos públicos cuyas políticas y prácticas del manejo físico de la información no estaban orientadas a facilitar el acceso de las personas a la misma.

El reconocimiento del acceso a la información como derecho humano ha ido evolucionando progresivamente en el marco del derecho internacional de los derechos humanos. El sistema interamericano de derechos humanos ha cumplido en ello un rol fundamental. Recientemente la Corte Interamericana de Derechos Humanos, marcó un hito jurisprudencial al constituirse en el primer tribunal internacional en reconocer que el acceso a la información es un derecho humano que forma parte del derecho a la libertad de expresión.

Sin duda, uno de los mayores logros en la historia de la humanidad siempre ha sido el desarrollo y reconocimiento de derechos y libertades del hombre, dado que desde el inicio de su existencia y por su propia naturaleza, ha sido considerado un ente con capacidad de razonamiento. Dicha facultad lo ha hecho acreedor a una serie de

derechos y prerrogativas que le han permitido vivir con libertad dentro de la sociedad. En tal virtud, se considera a dichas prerrogativas como fundamentales.

En tal sentido, los derechos constitucionales históricamente nacidos como una garantía de libertad de las personas y configurados como derechos subjetivos frente al Estado, al que se le exigía una abstención o ausencia de intromisiones en determinados ámbitos de libertad de los ciudadanos, así como el proporcionar ciertos datos que son de interés para los ciudadanos haciendo valer sus derechos de libertad.

Esto es, Derechos como la libertad ideológica y religiosa, la libertad personal y ausencia de detenciones, la inviolabilidad de domicilio, el secreto de las comunicaciones, la libertad de expresión y comunicación, la libertad de residencia y de circulación, incluso, el Derecho al honor y a la intimidad, tenían como principal amenaza a los poderes públicos.

Por tanto, con el reconocimiento constitucional de los derechos de la persona, el sometimiento del Estado al imperio de la ley y al principio de legalidad administrativa, así como el control judicial de sus actos por un poder judicial independiente, vendrían a limitar a los poderes públicos con el fin de asegurar unas esferas de libertad para los ciudadanos.

Desde esta visión clásica de los derechos fundamentales, el derecho a la protección de los datos personales y el acceso a la información pública, es también un derecho frente al Estado y frente a los poderes públicos, a los que se les puede exigir el respeto a una esfera personal que obliga a ambos a cumplir unos principios y a respetar unos Derechos en los tratamientos de datos por parte de los poderes públicos. Razón por la cual, en países latinoamericanos aportan no sólo el reconocimiento de unos derechos económicos y sociales inherentes al bienestar de los ciudadanos, que se unían ya a los derechos de la esfera personal tradicionales del Estado liberal y a los derechos políticos del Estado democrático, sino a la introducción en la dogmática de los derechos del concepto de derecho fundamental, que representa una superación de la visión de los derechos como algo meramente subjetivo.

Consecuencia de ello, en Guatemala es necesario impulsar reformas legislativas que garanticen facultades de control sobre las informaciones personales de los ciudadanos y la necesidad de incorporar prescripciones constitucionales que amplíen la tutela que recibe la privacidad.

Por tanto, al margen de las consideraciones que pueda ser objeto el reconocimiento del derecho fundamental a la protección de datos personales, en concordancia práctica con otros derechos constitucionales tales como el derecho a la protección de la dignidad humana, a la libertad individual, a la autodeterminación y el principio democrático, principios que han adquirido una nueva perspectiva en el Estado de Derecho, sirviendo de referencia para el resto de países latinoamericanos, contribuyendo para que sea más efectivo su reconocimiento respecto al tratamiento de los datos personales por parte de la administración pública.

Previo al estudio de ellos, resulta preciso conocer la transformación de la tradicional administración pública con la llegada de las nuevas tecnologías y que han contribuido al establecimiento de un equilibrio entre la protección de los datos personales frente a lo que hoy se conoce como administración electrónica.

1.1. Concepto

La palabra información es masivamente utilizada en distintas disciplinas, ámbitos y momentos que su significado se vuelve algo difuso.

¿Qué es la información? El Diccionario de la Real Academia Española, ofrece varias definiciones entre las que se puede destacar “Acción y efecto de informar”, “Oficina donde se informa sobre algo” y “Conocimientos así comunicados o adquiridos”.¹ Otra definición necesaria incluirla, es la tomada del autor Miguel de Moragas, donde define que el término información alude a un “conjunto de datos organizados de manera tal

¹ <http://buscon.rae.es/drae/>

que aportan un significado, sin esta condición de orden u organización, simplemente serían datos.

La información es una parte fundamental y necesaria en todo proceso comunicativo en cuanto que es significada por quien la recibe si existe entre receptor y emisor un código común.

La información es en cualquier caso el concepto que obtiene mayor atención en la actual ciencia moderna de la información.

La información conlleva, en sí misma, una parte teórica y otra práctica que en el pensamiento humano se presentan como separadas. La unificación que desemboca en la construcción definitiva del concepto de información, se da por la interacción dialéctica entre lo teórico y lo práctico”.²

En la Edad Media se conceptualizó a la información como una organización activa que dirige los modelos del pensamiento humano. Pero lo que marca la diferencia en los seres humanos, puesto que la información se encuentra en la naturaleza misma, es la posibilidad de crear y perfeccionar sistemas de símbolos con significados. Este es el origen del lenguaje, útil para la convivencia social. Puede pensarse en la información como la manera de exteriorizar la producción del pensamiento humano.

En la actualidad, la globalización permite el acceso a enormes volúmenes de información depositados en soportes cada vez más complejos, con increíbles posibilidades de almacenamiento y conexión con otras fuentes. Nos referimos a las bases de datos, las redes de transmisión de datos, Internet...Etc.

La información es un punto clave para todo desarrollo económico y social, permite altos grados de competitividad debido a la demanda permanente y porque esta se genera

² De Moragas Spa, Miguel, **Semiótica y comunicación de masas**, pág. 86.

cada vez más. En general y de una manera sumamente amplia se definen dos grandes tipos de información: la información pública y la información privada.

La información pública es un derecho consagrado que permite el control, monitoreo y participación del individuo social en los asuntos públicos, del Estado y de las instituciones gubernamentales. La información privada es aquella que no debería trascender a las personas que la manejan.

La información privada es inviolable sino medía una orden legal que justifique tal acción. Esta regulación a la ley en Guatemala debiera hacer énfasis que a nivel informático los administradores de sitios que solicitan información personal o privada a sus suscriptores o usuarios, estarán penados legalmente si la vendieran, expusieran o revelasen sin autorización.

Las disposiciones de la Ley de Acceso a la Información Pública son de orden público y de observancia general en el territorio de Guatemala. El Artículo nueve, numeral tres, de la Ley de Acceso a la Información Pública establece que “toda la información generada, administrada o en posesión de los Entes Públicos se considera un bien, accesible a cualquier persona en los términos y condiciones que establece esta Ley y demás normatividad aplicable. Esta sección promueve el Derecho de Acceso a la Información Pública.”

1.2. Clasificación

1.2.1. Tipos de información

Para efectos de este estudio los tipos de información que se estudiarán son los considerados de carácter público y los de carácter privado o personal. En el primero son los que el sujeto tiene o puede exponer y con libre albedrío como su nombre, edad, nacionalidad, Etc. los considerados como carácter personal son aquellos que por su naturaleza merecen un grado de mayor recelo o secretividad a menos que por orden

judicial sea el individuo obligado a revelarlos, entre esta información considerada como carácter personal se encuentra sus estados financieros, sus propiedades, sus gustos sexuales, sus ingresos económicos, Etc.

1.2.2. Conforme a doctrina

La eficiencia de una norma puede depender del estilo de redacción y contenido, así como la claridad y precisión que contenga la misma. El mayor problema de la presente Ley es la de establecer las excepciones, y proteger sólo aquellas que se establecen en la Constitución, especialmente a las contenidas en el Artículo 30 que hacen referencia a la seguridad nacional, en temas militares y diplomáticos.

El listado de excepciones o límites al acceso a la información pública es abundante, pero el mismo también responde a los límites que establece la Carta Magna, la cual contiene muchos elementos que protegen privilegios y prebendas de actores y sectores, especialmente los del sector económico y acciones militares.

Se considera importante tomar en cuenta lo que otros países han hecho en lo que respecta a esta materia y que consagran en sus Constituciones como derechos fundamentales de manera expresa el derecho al acceso de la información, entre estos países:

Constitución portuguesa (1976)

Artículo 268

2. Los ciudadanos tendrán derecho de acceso a los archivos y registros administrativos, sin perjuicio de lo dispuesto por la ley en materias relativas a la seguridad interna y externa, la investigación criminal y la intimidad de las personas.

Constitución española (1978)

Art. 105. La ley regulará:

b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

Constitución brasileña (1988)

Art. 5.

XXXIII – todos tienen derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general que serán suministradas dentro del plazo de ley, bajo pena de responsabilidad, salvo aquellas cuyo sigilo sea imprescindible para la seguridad de la sociedad o del Estado.

Constitución colombiana (1991)

Art. 74.

Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.

Constitución peruana (1993)

Art. 2.

5) A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

Constitución de la ciudad de Buenos Aires (1996)

Art. 26.

4° párrafo: Toda persona tiene derecho, a su solo pedido, a recibir libremente información sobre el impacto que causan o pueden causar sobre el ambiente actividades públicas o privadas.

1.2.3. Conforme a ley

En el Artículo 25 de la Ley de Acceso a la Información Pública de Guatemala, se establecen las clasificaciones de la información que es considerada como reservada, la misma “se hará mediante resolución de la máxima autoridad del sujeto obligado la que debe ser publicada en el Diario Oficial y debe indicar lo siguiente:

1. La fuente de la información;
2. El fundamento por el cual se clasifica;
3. Las partes de los documentos que se reservan;
4. El plazo de reserva que no será mayor de siete años; y,
5. El nombre de la autoridad responsable de su conservación.

Son nulas aquellas resoluciones que clasifiquen la información como confidencial o reservada si estas no llenan los requisitos establecidos en la presente ley. Será procedente el recurso de revisión.”

La Ley de Acceso a la Información Pública de Guatemala tiene por objeto transparentar el ejercicio de la función pública, garantizar el efectivo acceso de toda persona a la información pública en posesión de los órganos locales: Ejecutivo, legislativo, judicial y autónomos por ley, así como de cualquier entidad, organismo u organización que reciba recursos públicos. El ejercicio del derecho a la información comprende difundir, investigar y recabar información pública.

Establece como objetivos primordiales: Proveer lo necesario para que toda persona pueda tener acceso a la información pública gubernamental, mediante procedimientos sencillos, expeditos y gratuitos; Optimizar el nivel de participación comunitaria en la toma Pública de decisiones, y en la evaluación de las políticas públicas.

Garantizar el principio democrático de publicidad de los actos del gobierno, transparentando el ejercicio de la función pública, a través de un flujo de información oportuno, verificable, inteligible, relevante e integral; favorecer la rendición de cuentas,

de manera que se pueda valorar el desempeño de los sujetos obligados; mejorar la organización, clasificación y manejo de documentos en posesión de los entes públicos; contribuir a la democratización y plena vigencia del Estado de Derecho, así como a la transparencia y la rendición de cuentas de los entes públicos a través de la generación y publicación de información sobre sus indicadores de gestión y el ejercicio de los recursos públicos de manera completa, veraz, oportuna y comprensible.

1.3. Limitaciones

“En junio de 2003, la Asamblea General de la Organización de los Estados Americanos OEA reconoció la importancia del acceso a la información pública especificado en la Resolución AG/Res.1932 (XXXIII-O/03), en la cual reafirma la declaración del Artículo 13 de la Convención Americana donde se establece de que todos tienen libertad de procurar, recibir y difundir información. También sostuvo que el acceso a la información pública es un requisito del ejercicio mismo de la democracia. Como se observa, en el continente Americano el derecho de acceso a la información pública encuentra sólidos fundamentos políticos y jurídicos.

Entre los cuales también cabe mencionar el Principio sobre Libertad de Expresión No. 4 (“Principio No. 4”) de la Comisión Interamericana de Derechos Humanos (“Comisión Interamericana”), que también reafirma el Artículo 13 de la Convención Americana. El Principio No. 4, reconoce que el derecho a acceder a la información en poder del Estado es un derecho fundamental que sólo admite limitaciones excepcionales establecidas en forma previa mediante una ley, y agrega además esta declaración, que las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público.”³

Aunque la información que pretende sea de acceso público existen algunas limitantes para su obtención u acceso. Esto se debe a que alguna información puede poner en

³ Romero Silvera, Graciela, *Implicaciones jurídicas del desarrollo del derecho de acceso a la información pública, en el marco del derecho a la libertad de expresión y los derechos humanos*, págs. 162-163.

riesgo a la Nación por tal razón toda solicitud debe realizarse de conformidad con los principios que dicha información para que esta sea accesible para el público.

La Ley de Acceso a la Información Pública es un proyecto muy ambicioso, por tal razón en ella se estipulan los principios que toda persona tiene derecho a la libertad de información en poder de los organismos públicos, con sujeción únicamente a las disposiciones de esta ley.

Cualquier persona que haga una solicitud a un organismo público tendrá derecho, sin perjuicio de únicamente a las disposiciones establecidas en el Artículo 21 de dicha ley donde establece que “El acceso a la información pública será limitado de acuerdo a lo establecido en la Constitución Política de la República de Guatemala, la que por disposición expresa de una ley sea considerada confidencial la información considerada como reservada de conformidad con la presente ley y las que de acuerdo a tratados o convenios internacionales ratificados por el Estado de Guatemala tengan cláusula de reserva”.

Con la finalidad de fortalecer las capacidades de organizaciones y actores locales para promover el derecho de acceso a la información en Guatemala, la presencia ciudadana debiera realizar un monitoreo ciudadano a la Ley de Acceso a la Información Pública lo que contribuirá a un mejor conocimiento y aplicación de la misma en el país, lo cual tendría como valor agregado a que más gente se involucre en las acciones y decisiones que toman los gobiernos para dirigir el país.

Esta presencia activa debiera entrar a detalle para determinar si existen problemas logísticos, falta de presupuesto, problemas de archivo o de personal adecuado e incluso personal designado. Para que no existan problemas instrumentales que limiten el acceso a la información.

Siendo la información un catalizador de la participación social es importante que exista acceso a ella, pues quien tiene más y mejor información goza de mayores posibilidades

de participar e incidir en la toma de decisiones concernientes a políticas públicas y a la exigencia de una pronta impartición de justicia en temas y problemas propios del país.

Bajo dicho contexto, Guatemala debiera tomar modelos para la aplicabilidad de la Ley como lo han hecho en España y Argentina, entre otros. Con lo cual se podría sistematizar las lecciones aprendidas, sobre los avances y obstáculos que tuvieron dicho países en la comprensión y uso del derecho del acceso a la información, así como para conocer los intereses específicos de cada ciudadano en materia social y política.

Como en todo inicio, puede que existan ciertas dificultades presupuestarias que se refleja en la falta de personal especializado y específico para brindar información. A su vez, este problema podría derivar la falta de organización de las entidades de la administración pública y para algunos resulta causa importante de que la información no sea brindada a los solicitantes en tiempo, a pesar de que existen plazos para tal efecto.

El proceso de adoptar una cultura de transparencia en Guatemala ha sido lento, pues conlleva todo un cambio cultural, y la voluntad política para informar al ciudadano no ha sido muy clara hasta ahora, según algunas notas periodísticas publicadas en algunos medios escritos. Por otro lado, los grandes grupos de la sociedad guatemalteca no ejercen el derecho de acceso a la información pública pues no saben que lo tienen o no encuentran una aplicación práctica en él, y solo los sectores de amplio nivel educativo como académicos, medios de comunicación, empresarios, abogados y algunos miembros de la sociedad civil han hecho suyo este derecho instrumental, para exigir la rendición de cuentas, ejercer derechos o cumplir obligaciones en diferentes actividades de la vida pública y privada, teniendo impacto en los procesos de formación de la opinión pública.

Algunas instituciones de gobierno están creando portales web los cuales son sinónimo de transparencia y son vistos como un medio eficaz para dar a conocer la información relativa a la administración pública. En este sentido, la creación de páginas web es un

indicador de implementación de la Ley. Sin embargo, algunos especialistas en el tema indican que no toda la información que debería ser expuesta figura en los portales. Además, estos expertos creen que los portales cumplen un papel publicitario más no necesariamente informativo, y que la información no está debidamente organizada ni actualizada.

La Ley de Acceso a la Información Pública, también tiene un inciso que refiere al acceso a la información ante violaciones o delitos de derechos humanos, aunque con un alcance más acotado. Expresa el inciso inicial del Artículo 12 que “Las sentencias condenatorias dictadas con autoridad de cosa juzgada por delitos de derechos humanos y lesa humanidad;” el cual se sopesa con el Artículo 24 en el cual se establece que “En ningún caso podrá clasificarse como confidencial o reservada la información relativa a investigaciones de violaciones a los derechos humanos fundamentales o a delitos de lesa humanidad.”

El fundamento del acceso a la información pública consagrado en algunos de los artículos analizados, ya no es sólo la transparencia o la publicidad de la información pública que inspira a la ley de acceso en general, sino la protección de la dignidad inherente al ser humano que se encuentra en la base de la tutela y protección de los derechos humanos. Además, el reconocimiento y la difusión por parte del Estado de los datos que son hechos históricos, sociales, culturales, económicos, etc., de una sociedad, para darlos a conocer a las personas y a la sociedad que ha sido víctima, es imprescindible no sólo para el desarrollo de las investigaciones sino para el debate de los hechos y el fomento de la participación política. Éstas y otras condicionantes sociales colaboran con el ejercicio de una ciudadanía activa y responsable.

Por ser Guatemala un país pluricultural, necesita una identidad definida, la identidad de una nación implica, entre otras cosas, “preguntarse y responder de manera más o menos permanente quiénes somos, de dónde venimos, hacia dónde vamos. Y para responder se necesita el mapa de la geografía social y política, se necesita una historia

conocida,⁴ una historia oficial común a todos, una memoria colectiva y ello también constituye un derecho humano tanto en su dimensión colectiva como individual.

Por lo antedicho a pesar que en la ley se establece en el artículo 42 del Decreto 57-2008, Ley de Acceso a la Información Pública, que “Presentada y admitida la solicitud la unidad de información donde se presentó, debe emitir resolución dentro de los diez días siguientes” El procedimiento estipulado para solicitar información puede ser un factor que limita el cumplimiento de la Ley, debido a los problemas que identifican los ciudadanos. Básicamente, esta situación radica en la incertidumbre generada por no saber si la solicitud será atendida, por ser reservada porque no hay ninguna regulación que exprese como definitiva cual es la información reservada y confidencial.

En definitiva, las restricciones al acceso a la información deben ser muy limitadas y sólo previstas por ley, establecido en el Artículo 21, Ley de Acceso a la Información Pública. En general, los expertos en el tema entienden que las áreas reservadas al acceso sólo se deben fundar en la protección de la seguridad nacional o en el derecho a la intimidad de las personas cuyos datos estén en la órbita de los poderes estatales. Por lo tanto casi siempre cuando se refiere a la seguridad nacional se alude a la información reservada y cuando se refiere a la protección de la intimidad de las personas se alude a la información confidencial. En casos de información que posee o controla el Estado, la restricción es la excepción, la cual además debe ser fundamentada legalmente por quien niega el acceso en la resolución emitida.

1.4. El impacto del uso de la ley de acceso a la información pública

Antes de entrar a profundidad acerca del tema del Impacto que ha tenido la Ley de Acceso a la Información en Guatemala se hace necesario estar en concordancia con Gettell, en torno al pensamiento de Platón: “[...] sostiene la teoría de que no puede concebirse el Estado fuera de los individuos que lo integran [...] él consideraba a las

⁴ Luis Pérez, Aguirre, **Ponencia, el Uruguay impune y la memoria social en el Tribunal permanente de los pueblos**, págs. 127-136.

personas indispensables para la formación, mantenimiento y funcionamiento del Estado, en tal sentido es necesaria una participación social, que busque el funcionamiento de las instituciones políticas, y que éstas, a su vez, reflejen el sano desarrollo de la Sociedad”.⁵ Esto es lo que se busca al hablar de Acceso a la Información y el impacto de transparencia que se ha tenido en Guatemala, para lograr una inclusión de la sociedad en la formación de políticas públicas y de aportaciones sociales encaminadas a bien dirigir la política y economía del país.

Desde la promulgación de la Ley de Acceso a la Información Pública, se han propiciado cambios favorables para la promoción y defensa de la transparencia pública. Esta Ley ha sido introducida paulatinamente en las instituciones de la administración pública, gracias al trabajo complementario que realiza la prensa junto a la sociedad civil.

El conocimiento de la Ley de Acceso a la Información Pública es relativo a las funciones y ocupaciones de los sujetos en algunos casos. La existencia de la Ley es conocida por muchos, pero no su contenido, funciones o disposiciones específicas.

El conocimiento de la Ley es diferente de acuerdo a los actores públicos, dentro de las instituciones y en la sociedad civil. En el primer caso, quienes están directamente vinculados al tema de la información tienen un conocimiento más profundo, mientras que aquellos que no tienen una función directa con dicho tema pueden conocer la nomenclatura, pero no los contenidos, plazos y funciones específicas que indica la Ley y es a partir de tal desconocimiento donde puede entrar el conflicto la aplicabilidad de la misma.

Los miembros de la sociedad civil que constantemente demandan información, por ejemplo son los periodistas, y se concentran en el tema de los plazos y tienen un carácter sustancialmente instrumental. Lo que se muestra es una diferencia entre el conocimiento directo de la Ley y el conocimiento del derecho que la ampara. Algunos funcionarios y miembros de la sociedad civil, si bien indican no conocer la ley o

⁵ Gettell, R., *El pensamiento político en Grecia. Historia de las ideas políticas*, pág. 93.

conocerla sólo superficialmente, reconocen que sí están informados y plenamente conscientes de que tienen derecho a solicitar la información pública como medio de control y fiscalización. El desconocimiento de la Ley y su contenido jurídico, no implica el desconocimiento del derecho a demandar y acceder a la información, esto puede ser un impacto negativo para la aplicabilidad y el fin con el cual la esta Ley fue creada.

Los funcionarios del Estado, los periodistas y ciudadanos en general conocen la existencia de los instrumentos que facilitan el acceso a la información pública. Uno de estos elementos son los portales web. Esto indica que si bien algunos no conocen la nomenclatura del derecho mismo o la Ley en su contenido profundo, sí tienen conciencia de la existencia de sus instrumentos prácticos. En muchos casos, sin embargo, no conocen la información que contiene, la profundidad de la misma o sus funciones específicas.

Hay poco conocimiento sobre las sanciones que podría acarrear el incumplimiento de la Ley de Acceso a la Información Pública. “El único caso de sanción que hasta hoy día se conoce fue la dictada a un Ministro de Educación en febrero de 2010. La Corte de Constitucionalidad dicto la sentencia de destitución a dicho funcionario por no acatar un fallo judicial”.⁶ Es decir, que dichas sanciones no están tipificadas en la ley, pero según el Artículo 66 de esta Ley establece que “Incorre en el delito de retención de información el funcionario, servidor público o cualquier persona responsable de cumplir la presente ley, que en forma arbitraria o injustificada obstruya el acceso del solicitante a la información requerida. Será sancionado con prisión de uno a tres años, con inhabilitación especial por el doble de la pena impuesta, y multa de 10,000.00 a 50,000.00 Quetzales.

La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la retención de la información.” En este caso la sanción no se dio explícitamente conforme a la ley, sin embargo, con la destitución del funcionario dio el indicio que con la presente Ley se

⁶ http://www.prensalibre.com.gt/edicion_impresa/pdf/, pág. 2.

quiere hacer transparente la sanción por el actuar de los funcionarios y servidores públicos aunque no en su totalidad, como se dio en este caso.

Un sector de la ciudadanía suele usar la Ley como un instrumento que garantiza su derecho a acceder a información. En efecto, si se les niega el acceso o hay una demora en la entrega, saben que pueden optar por vías legales para denunciar la retención o la negación de la información. Sin embargo, esto permite también mal utilizar la Ley, en algunos casos, podría generarse un mecanismo de presión para conseguir información reservada o para generar canales informales de entrega de información.

El mayor problema radica en que si no se conoce la legislación o no se pueden aprovechar los mecanismos que la Ley tutela para el ejercicio de este derecho, una Ley de esta naturaleza realmente sirve de poco. Destinar recursos para socializar el conocimiento y uso de la Ley es parte importante, así como otorgar facultades para que alguien promueva la cultura ciudadana por todos los medios educativos posibles, pero si la misma no se aplica como tal esta inversión de recursos se volvería un gasto más para el país.

La importancia de esta Ley es la transparencia, debido a que no es sólo un elemento que proviene de la voluntad del poder público, sino se ha convertido en una exigencia por parte de los ciudadanos, a quienes también les interesa ejercer su derecho contralor sobre el uso de los recursos que ellos proveen al Estado a través del pago de Impuestos. Además, esta acción de querer transparentar las acciones públicas coadyuva a legitimar la administración, así como a la existencia de mecanismos de rigor y de eficiencia en la acción administrativa.

El mayor problema de la aplicabilidad de las Leyes en Guatemala siempre ha sido el desconocimiento. Antes y durante la entrada en vigencia de esta norma, lo ideal hubiera sido que se iniciaran campañas ciudadanas para promover la cultura de transparencia y los procesos de solicitud de información y se hicieran públicos los

formatos de solicitud, procedimientos, plazos, entre otros, lo que beneficiaría a la ciudadanía, para que se involucre en la participación política del país.

Es importante y necesario que las organizaciones de la sociedad civil reconozcan a la Ley de Acceso a la Información Pública como un instrumento útil e indispensable para su quehacer cotidiano y repliquen el conocimiento para contribuir a que los ciudadanos se apropien de este derecho fundamental que sin duda impulsa la construcción de sociedades más justas, equitativas y corresponsables en la gestión de asuntos públicos y que coadyuva al fortalecimiento del patrimonio social y la vida democrática del país.

Hasta ahora el gobierno de Guatemala, ha realizado considerables esfuerzos para dar cumplimiento a sus obligaciones en materia de transparencia; pero el cumplimiento de esta ley es muy heterogéneo en las diferentes dependencias del Estado. Estas dependencias se han enfocado a cumplir con la norma, más la información que otorgan al ciudadano no siempre es de calidad ni satisface sus demandas según lo indica la prensa.

Es de vital importancia que la sociedad guatemalteca esté interesada en participar con capacidad de transformar los datos en información relevante que sirva para entender la complejidad técnica del gobierno y se pueda establecer una interlocución constructiva con las distintas entidades del Estado, dejando a un lado la actitud enjuiciadora y castigadora que la transparencia puede arrastrar consigo.

Para lograr un impacto positivo se debe mejorar la información que se maneja en los medios de comunicación: y que la prensa tome responsablemente su labor de divulgación e información y no de amarillismo y simplificación, porque no se trata de castigar a persona alguna sino de encarrilar al país a un mejor estado de vida.

El Estado debe promover y encaminar la divulgación de la información en una verdadera simplificación administrativa, además de una selección de la información a transparentar ya que es imposible pretender el universo de información completamente transparente, de lo contrario seguiremos perdidos solamente en un mar de datos.

Además de debe crear la vinculación de la Ley de Acceso a la Información Pública con otras leyes existentes para fortalecerla, y hacer que esta Ley tenga vida propia para que su cumplimiento sea más efectivo, además del Habeas Data, que es el mayor problema que existe en la actualidad.

Promover el fortalecimiento de las relaciones entre la sociedad civil y gobierno con la finalidad de construir políticas públicas en beneficio de la sociedad y para generar un ambiente de mayor confianza y credibilidad entre estos sectores, la Ley por si misma sólo son palabras escritas, pero este fortalecimiento será la piedra angular de la Ley.

Se debe realizar un monitoreo y contraloría ciudadana a esta nueva Ley de transparencia pública pues hoy por hoy se mide su eficacia cuantitativamente, basándose en estadísticas que indican cuantas solicitudes han sido ingresadas a las dependencias, cuantas contestadas dentro de los plazos que marca la ley entre otras, pero no hay ningún mecanismo u organismo que este evaluando la calidad de la información, y esto se puede conocer a través de estos monitoréos así como insumos para realizar estrategias de incidencias para el fortalecimiento y mejoras de las demás leyes existentes en el país.

Finalmente es importante mencionar que es tarea de los ciudadanos que solicitan información el denunciar anomalías y exigir que se les otorgue información de calidad, y que para llegar a la rendición de cuentas e impartición de justicia no basta con apropiarse del derecho de acceso a la información.

Con lo anterior, se quiere decir que no es bueno generar tantas expectativas sobre un derecho y una herramienta para acceder a la información pública pues mientras no se refuercen otros sectores como el sistema judicial, el Habeas Data, por mencionar algunos, no se lograra avances significativos en materia de rendición de cuentas, lucha contra la corrupción e impartición de justicia.

CAPÍTULO II

2. Derecho de la informática

Antes de entrar a detalle en lo que respecta al derecho a la informática se hace necesario explicar algunos conceptos que serán de vital importancia para la comprensión del tema.

Primeramente se cuestiona si ¿Constituye el derecho informático y la informática jurídica verdaderas ciencias? Para dar respuesta a estas preguntas es necesario hacer un análisis de los conceptos: Ciencia, informática jurídica y derecho informático.

¿Qué es una Ciencia? Según la Real Academia Española la Ciencia es: "El conocimiento cierto de las cosas por sus principios y causas. //1. Conjunto de conocimientos obtenidos mediante la observación y el razonamiento, sistemáticamente estructurados y de los que se deducen principios y leyes generales...//3. Habilidad, maestría, conjunto de conocimientos en cualquier cosa".⁷

Sin duda alguna, que tanto la informática jurídica como el derecho informático constituyen conocimientos, principios, doctrinas, que catalogan a estas disciplinas como ciencias, que tienen como marco estricto a la iuscibernética y como marco amplio a la cibernética.

"El derecho informático por así decirlo es la otra cara de la moneda. En esta cara se encuentra por un lado a la informática jurídica, y por otro entre otras disciplinas el derecho informático; que ya no se dedica al estudio del uso de los aparatos informáticos como ayuda al derecho, sino que constituye el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la

⁷ www.rae.es/rae.html

aplicación y desarrollo de la informática. Es decir, que la informática en general desde este punto de vista es objeto regulado por el derecho.

Ahora bien, la informática jurídica constituye una ciencia que forma parte del ámbito informático, demostrando de esta manera que la informática ha penetrado en infinidad de sistemas, instituciones, Etc., prueba de ello es que ha penetrado en el campo jurídico para servirle de ayuda y servirle de fuente. Por lo tanto, la informática jurídica puede ser considerada como fuente del derecho, criterio propio que tal vez encuentre muchos tropiezos debido a la falta de cultura informática que existe en Guatemala.

Al penetrar en el campo del derecho informático, se obtiene que también constituye una ciencia, que estudia la regulación normativa de la informática y su aplicación en todos los campos. Pero, cuando se dice derecho informático, entonces se analiza si esta ciencia forma parte del derecho como rama jurídica autónoma; así como el derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal es el caso de la civil, penal y contencioso administrativa".⁸

¿Es el derecho informático una rama del derecho? "Al respecto, según encuentros sobre informática realizadas en facultades de derecho en España a partir de 1987, organizados por ICADE, siempre surgían problemas a la hora de catalogar al Derecho Informático como rama jurídica autónoma del derecho o simplemente si el derecho informático debe diluirse entre las distintas ramas del derecho, asumiendo cada una de estas la parte que le corresponde.

Por exigencias científicas, por cuanto un conjunto de conocimientos específicos conllevan a su organización u ordenación, o por razones prácticas que llevan a la separación del trabajo en vías de su organización, se encuentra una serie de material de normas legales, doctrina, jurisprudencia, que han sido catalogadas y ubicadas en diversos sectores o ramas. Dicha ordenación u organización del derecho en diversas ramas, tiene en su formación la influencia del carácter de las relaciones sociales o del

⁸<http://informatica-derecho-juridico/informatica-derecho-juridico.shtml#constituy>

contenido de las normas, entonces se van formando y delimitando en sectores o ramas, como la del derecho civil, penal, constitucional, contencioso administrativo..., sin poderse establecer límites entre una rama jurídica y otra por cuanto, existe una zona común a todas ellas, que integran a esos campos limítrofes. De manera que esta agrupación u ordenación en sectores o ramas da origen a determinadas Ciencias Jurídicas, que se encargan de estudiar a ese particular sector que les compete".⁹

Para analizar esta situación, es necesario mencionar las bases que sustentan a una rama jurídica autónoma, y al respecto se encuentran:

Una legislación especificada (campo normativo).

Estudio particularizado de la materia (campo docente).

Investigaciones, doctrinas que traten la materia (campo científico).

Instituciones propias que no se encuentren en otras áreas del derecho (campo institucional).

Ahora bien, ¿Qué sucede con el derecho informático? "Generalmente el nacimiento de una rama jurídica surge a consecuencia de cambios sociales reflejados en las soluciones normativas al transcurso de los años. Pero resulta que, en el caso de la informática no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo, se lograron de esta manera sociedades altamente informatizadas, que sin la ayuda actual de la informática colapsarían.

No obstante, a pesar de esta situación existen países desarrollados como España en los que sí se puede hablar de una verdadera autonomía en el derecho informático, haciendo la salvedad de que ésta ciencia como rama jurídica apenas nace y se está desarrollando, pero se está desarrollando como una rama jurídica autónoma.

⁹ Ibid

En el caso de Venezuela, son muy pocos los sustentos que se encuentran para el estudio de esta materia, tal vez su aplicación se limita fundamentalmente a la aparición de libros con normativas (doctrina), y comentarios de derecho informático”.¹⁰

Pero tal vez, sea más fácil para los abogados buscar esta normativa en las otras ramas del derecho, por ejemplo; acudirían al Código Civil para ver lo relativo a las personas (protección de datos, derecho a la intimidad, responsabilidad civil). Conforme a lo establecido en el Artículo 274 “D”, Código Penal, Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un bando de datos o un registro informático con datos que puedan afectar la intimidad de la persona” adicional a lo regulado en el Código Civil, establece en el Artículo 1645, que toda persona que cause daño o perjuicio a otra, sea intencionalmente, sea por descuido o imprudencia, está obligada a repararlo, salvo que demuestre que el daño o perjuicio se produjo por culpa o negligencia inexcusable de la víctima”.

Resulta, sin embargo, que esta situación no se acopla con la realidad informática del mundo, ya que existen otras figuras como los contratos electrónicos y documentos electrónicos, que llaman a instituciones que pertenezcan a una rama autónoma del derecho.

“En este orden de ideas, es menester entonces concluir que en el derecho informático si existe legislación específica, que protege al campo informático. Tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero si existe en el derecho informático, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de nuestras naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

¹⁰ **Ibib**

Con respecto a las instituciones propias que no se encuentren en otras áreas del derecho (campo institucional), se encuentra el contrato informático, el documento electrónico, el comercio electrónico, entre otras, que llevan a la necesidad de un estudio particularizado de la materia (campo docente), dando como resultado las Investigaciones Y doctrinas que traten la materia (campo científico). En efecto, se pueden conseguir actualmente grandes cantidades de investigaciones, artículos, libros, e inclusive jurisprudencia que esté enmarcada en la interrelación entre el derecho y la informática, como se ha constatado en los Congresos Iberoamericanos de Derecho e Informática”.¹¹

2.1. Información pública en la era informática

“La información pública no es más que la información en poder de los sujetos obligados contenida en los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los mismos podrán estar en cualquier medio sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico y que no sea confidencial ni estar clasificado como temporalmente reservado”. Dicha información está contemplada en la Constitución Política de la República de Guatemala en su Artículo 31.

El derecho a la información pública en la República de Guatemala está actualmente relacionado con la transparencia, la rendición de cuentas y el acceso a la información del sector público; lo que significa abrir el ejercicio del gobierno a la ciudadanía, para que ésta sea capaz de evaluar a sus representantes, de ejercer con mayor precisión sus opiniones respecto de los asuntos que le conciernen directamente y de brindarle la

¹¹ **ibid**

posibilidad de incidir y participar en las decisiones de política pública que, en última instancia, se diseñan para el beneficio de todos los ciudadanos.

En su Artículo 10, de la Ley de Acceso a la Información Pública establece tácitamente, “que la rendición de cuentas es la obligación de informar periódicamente sobre las acciones públicas, es decir: qué se hizo, cómo, con qué y para qué se hizo. Entonces el acceso a la información se traduce en prerrogativas que permiten a la ciudadanía tener conocimiento sobre documentos y datos que son generados y administrados por el sector público, siempre que medie solicitud expresa”.

El reconocimiento del derecho a la información en Guatemala, bajo el marco legal de la Ley de Acceso a la Información Pública, permite hablar de cierta evolución en el desarrollo de la democracia política. En ésta norma se busca la construcción de un gobierno transparente; se pretende que a pesar de las contradicciones y conflictos de intereses que existen entre los actores e instituciones que intervienen en la vida pública, éstos se manejen bajo el principio de transparencia, lo que hará prevalecer los fundamentos de la democracia.

En la mayor parte del mundo la ciudadanía es la primera que exige una reglamentación sobre derecho a la información. No basta con recibir información educativa, cultural o entretenimiento, de alta o ínfima calidad, quiere hacerse escuchar para contribuir en la participación política, la conciencia cívica y hacer nuevas propuestas en la gobernabilidad del país.

El acceso a la información es una instancia necesaria para la participación ciudadana y la protección de los derechos civiles, dado que sin información adecuada, oportuna y fidedigna, solamente podrían ser considerados como datos muertos.

A pesar de las mejoras que se están dando en las normas que regulan las el acceso a la información pública, es preocupante cómo el crimen organizado se está involucrando en la obtención de información aprovechando este beneficio como en una nota periodística donde entre los delitos más recurrentes están los informáticos como son

“las extorciones por medio de correo electrónico y mensajes de texto. Hay que tomar en cuenta que la informática también llegó a los aparatos de telefonía móvil, los cuales dejan un rastro a través del sistema informático de la empresa de telefonía que presta el servicio”.¹²

La reciente ley aprobada en el 2008 de acceso a la información pública a los servicios públicos y sobre reutilización de la información del sector público se suman a un conjunto de disposiciones que han venido a regular, dentro del bloque constitucional debieran también regular la protección jurisdiccional de los derechos fundamentales de la persona; el régimen jurídico de las administraciones públicas y del procedimiento administrativo; los secretos oficiales; las telecomunicaciones; el derecho al honor, la intimidad personal y familiar; la utilización de técnicas electrónicas, informáticas y telemáticas por la administración del Estado.

Además se debieran contemplar todos los servicios de información administrativa; la protección de datos de carácter personal; los registros y las notificaciones telemáticas así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos y comunicación institucional, el derecho de petición; la calidad en la administración del Estado y la radio y la televisión.

La información pública es, por su volumen, por sus utilidades y por sus funciones, la que puede orientar de una manera decisiva el proceso de aplicación de las tecnologías de la información al desarrollo económico, social y democrático de nuestro país.

Esta función central de cualquier organización moderna en sus diferentes manifestaciones, la comunicación exterior, la información pública, la información institucional, la información general y particular a los ciudadanos está confluyendo en el uso de los mismos canales y medios. Solo podrán fundamentarse de manera sólida en la sociedad de la información, caracterizada por la eclosión de la red de Internet, la revolución de las telecomunicaciones (telefonía móvil, televisión digital...) y el creciente

¹² **En Internet todo queda registrado**, pág. 10, Prensa Libre (Guatemala), Año LIX, No. 19,473, lunes 1 de febrero de 2010, Guatemala.

papel de los medios de comunicación social sobre una estructura de sólidos Unidades de información pública servidos por profesionales de la gestión informativa.

2.2. La informática y el derecho

Entre el derecho y la informática se podrían apreciar dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la informática jurídica. Pero al considerar a la informática como objeto del derecho, se hace alusión al derecho de la informática o simplemente derecho informático.

La cibernética juega un papel bastante importante en estas relaciones establecidas en el párrafo anterior. Por cuanto se sabe que la cibernética es la ciencia de las ciencias, y surge como necesidad de obtener una ciencia general que estudie y trate la relación de las demás ciencias.

De esta manera, se tiene a la ciencia informática y por otro lado a la ciencia del derecho; ambas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el derecho en su aplicación, es ayudado por la informática; pero resulta que ésta debe de estar estructurada por ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas informáticas; así pues, nace el derecho informático como una ciencia que surge a raíz de la cibernética, como una ciencia que trata la relación derecho e informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer, regular las acciones, procesos, aplicaciones, relaciones jurídicas, en su complejidad, de la informática. Pero del otro lado encontramos a la informática jurídica que ayudada por el derecho informático hace válida esa cooperación de la informática al derecho.

La informática no puede juzgarse en su simple exterioridad, como utilización de aparatos o elementos físicos electrónicos, pura y llanamente; sino que, en el modo de proceder se crean unas relaciones inter subjetivas de las personas naturales o jurídicas y de entes morales del Estado, y surgen entonces un conjunto de reglas técnicas

conectadas con el Derecho, que vienen a constituir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la Ciencia informática, con autonomía propia.

Esos principios conforman las directrices propias de la institución informática, y viene a constituir las pautas de la interrelación nacional-universal, con normas mundiales supra nacionales y cuyo objeto será necesario recoger mediante tratados públicos que hagan posible el proceso comunicacional en sus propios fines con validez y eficacia universal.

2.3. La informática actual

“Cuando nos asomamos al fenómeno de la denominada Era Digital es inevitable llegar a la conclusión que todas aquellas historias de ciencia-ficción creadas por las mentes brillantes de Bradbury, Asimov y Verne, entre muchos otros, no sólo han sido confirmadas, sino que resultan, a poco que se efectúe el contraste respectivo, anacrónicas e ingenuas. Las posibilidades que ofrecen la biotecnología, la nanotecnología y la ingeniería genética son ilimitadas y plantean numerosos dilemas éticos, porque, por un lado, arrastran al hombre a un futuro donde se dispondrá de tiempo para hacer solamente las cosas placenteras, descartando las faenas laborales que tanto tiempo nos insumen y, en no pocas ocasiones, nos molestan, pero, por otro, se rompen límites morales: clonación de seres humanos, patentamiento de la codificación de las cadenas de ADN de determinadas partes del cuerpo humano con fines comerciales (a partir de la decodificación del genoma humano), desarrollo de sistemas de agentes inteligentes (IA -inteligencia artificial-) que potencialmente tienen capacidad de reemplazar a los expertos humanos en las más diversas áreas profesionales y, en el caso del derecho, podrían -por definición- analizar un caso determinado y emitir una decisión como lo haría un juez.

Sin embargo se trata de una incipiente tecno-era, porque el punto culminante de esta tercera revolución industrial tendrá lugar (y en muy poco tiempo) con la definitiva

expansión de la inteligencia artificial, la bio-tecnología, la genética y la robótica influyendo en todas las áreas humanas”.¹³

Tomando el pensamiento de Manuel Castells experto sociólogo, señala que “las consecuencias de este paradigma tecnológico también afectan y modifican la estructura social y económica, donde se observan las llamadas Economía Informacional (la capacidad de generación y manipulación de infraestructuras informacionales son decisivas para el desarrollo y expansión de las empresas), la Economía Red (descentralización de las grandes empresas y formación de redes o alianzas con pequeñas y medianas empresas que funcionan como auxiliares de aquéllas) y la Economía global o Globalización a secas (donde, en realidad, todos las áreas se encuentran subordinadas a este fenómeno: trabajo, comunicaciones, mercados financieros, cultura, Etc.)”.¹⁴

“Los frutos de estos cambios son naturalmente ambiguos: se crea un proceso donde la información está al alcance de todos (en Internet no sólo fluye la información, sino la sociedad misma), verificándose terribles impactos en lo que atañe a la difusión de la producción cultural y un rediseño de la arquitectura de los negocios y la industria. Sin embargo, el modelo económico neoliberal o post-capitalista globalizado, ha generado situaciones de exclusión e injusticia social a nivel mundial, cuya tendencia pareciera no ceder, destacándose el nuevo escollo, frente a la realidad de los países emergentes, que presentan las nuevas tecnologías de la información, las que, a diferencias de otros inventos (radio, televisión), requieren, como presupuesto mínimo indispensable, la alfabetización de los usuarios”.¹⁵

“La informática nos rodea y es una realidad incuestionable e irreversible. Está en casi todos los aspectos de la vida del hombre. Desde los más triviales hasta los más sofisticados. Sin la informática las sociedades actuales colapsarían, generándose lo que se conoce como computer dependency.

¹³ <http://www.delitosinformaticos.com/propiedadindustrial/auditoria.shtml>

¹⁴ Castells, Manuel, **La ciudad informacional. Tecnología de la información, estructuración económica y el proceso urbano-regional**, pág. 19.

¹⁵ **Ibid**

La informática se presenta como una nueva forma de poder, que puede estar concentrado o difuminado en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva forma de energía, si se quiere intelectual, de valor inconmensurable, que potencia y multiplica de manera insospechada las posibilidades de desarrollo científico y social, erigiéndose en patrimonio universal de la humanidad¹⁶. Sería muy difícil comprender el grado de poder de la informática, una comparación entre la civilización con escritura y la civilización sin ella, en la actualidad esto es inadmisibile.

2.4. Procesamiento de datos

“En la informática, un modelo de datos es un lenguaje utilizado para la descripción de una base de datos. Por lo general, un modelo de datos permite describir las estructuras de datos de la base (el tipo de los datos que incluye la base y la forma en que se relacionan), las restricciones de integridad (las condiciones que los datos deben cumplir para reflejar correctamente la realidad deseada) y las operaciones de manipulación de los datos (agregado, borrado, modificación y recuperación de los datos de la base).

En un enfoque más amplio, un modelo de datos permite describir los elementos que intervienen en una realidad o en un problema dado y la forma en que se relacionan dichos elementos entre sí.

La clasificación de los modelos de datos se realiza de acuerdo al nivel de abstracción. Los modelos de datos conceptuales son aquellos que describen las estructuras de datos y restricciones de integridad. Se utilizan durante la etapa de análisis de un problema dado y están orientados a representar los elementos que intervienen y sus relaciones.

¹⁶ **ibid**

Los modelos de datos lógicos se centran en las operaciones y se implementan en algún manejador de base de datos.

Por último, podemos mencionar a los modelos de datos físicos, que son estructuras de datos a bajo nivel implementadas dentro del propio manejador¹⁷.

2.5. Nuevos enfoques en la vida privada

“Podemos señalar que este panorama afecta al derecho, como instrumento regulador de las relaciones humanas en procura del orden social, pudiendo formularnos, entonces, algunos interrogantes: ¿Puede ajustar las instituciones jurídicas vigentes a estos fenómenos o, por el contrario, es necesario impulsar la creación de nuevas normas?, ¿Cuáles son los nuevos intereses colectivos que deben ser objeto de tutela jurídica?, ¿Es necesario el desarrollo de una nueva rama autónoma del derecho, atendiendo muy especialmente, al valor que posee la información en la sociedad actual?

Más allá de las discusiones teóricas que inevitablemente conllevan las preguntas supra referidas y que, en su mayoría, exceden el marco del presente trabajo, es necesario buscar fórmulas o mecanismos efectivos para solucionar los problemas que acarrearán el uso y la proliferación de las nuevas tecnologías, sin perjuicio de estudiar, paralelamente, el nuevo paradigma del conocimiento y la sociedad toda que impone la realidad actual.

Los problemas surgen del nuevo espectro de fenómenos de cierta complejidad tecnológica que no parecen encontrar adecuada solución ni en el ordenamiento jurídico vigente ni en las viejas elaboraciones doctrinales: el teletrabajo (esta curiosa modalidad de transpolar la oficina al hogar para el desempeño laboral) ¿Puede identificarse con la jornada laboral?, ¿Cómo establecer si existe un abuso por parte del empleador?, ¿El

¹⁷ <http://definicion.de/modelo-de-datos/>

software, incluido actualmente en una Ley de Propiedad Intelectual, puede identificarse ontológicamente con la obra artística?, ¿Cuál es el régimen de responsabilidad que corresponde aplicar a los proveedores de Internet según el tipo de servicio que prestan?, ¿Es correcto que se le imponga el deber de controlar lo que publica o difunde el usuario?, ¿Podría hablarse de un dolo general en la conducta del programador que diseña un virus o bomba lógica para enviarlo a un conocido o con fines experimentales, pero finalmente se disemina infectando la computadora de otras personas?, ¿De aceptarse la tentativa, es acabada o inacabada?, ¿La información, como entidad lógica, es susceptible de ser apropiada en los términos del delito de hurto, cuando la víctima sigue conservando la disposición sobre la información y no media afectación a su patrimonio?, ¿Cuál es el acto voluntario expresado en la celebración de un contrato cuándo el mismo constituye simplemente un doble clic? Continuar exponiendo estos problemas resulta abrumador y por cierto, interminable“.¹⁸

“Debe apuntarse, en lo que atañe al desarrollo y evolución del derecho informático, que en aquellos países donde el fenómeno de la informática se encuentra masificado, es decir, donde la mayoría de la población tiene acceso real a los sistemas de información, se habla del comienzo de una verdadera autonomía en esta área. No es posible desconocer, por otra parte, que, tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero sí existe en el ámbito del derecho informático, en el orden mundial, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos y leyes especiales que promueven los entes legislativos con la finalidad de proveer al contralor y encuadre legal de los instrumentos o medios informáticos.

Sin embargo, aceptando la necesidad del desarrollo del derecho informático como rama autónoma, el caso de Guatemala que se encuentra en la actualidad bastante lejos de lograr tal autonomía, habida cuenta que, en concordancia con la doctrina mayoritaria, es necesario que concurren cuatro aspectos: autonomía legislativa, autonomía jurisprudencial, autonomía académica y autonomía científica“.¹⁹

¹⁸ <http://delitosinformaticos.com/trabajos/hacking.pdf>

¹⁹ **Ibid**

Si bien se ha aludido a las tremendas posibilidades de la informática como instrumento de desarrollo económico-social y cultural y advertido acerca de algunas de sus consecuencias negativas, de la utilización perversa de las nuevas tecnologías de la información o, si se quiere, en aquellas nuevas conductas disociales que ameritan la intervención del Derecho Penal. Naturalmente que, frente a un fenómeno de tal magnitud como el que se describe, es imposible que la criminalidad quedara exenta del impacto de la tecnología informática.

Según expertos en tecnología, señalan que la informática abre nuevos horizontes al delincuente, incita su imaginación, favorece su impunidad y potencia los efectos del delito convencional. Y a ello contribuye la facilidad para la comisión y encubrimiento de estas conductas delictivas y la dificultad para su descubrimiento, prueba y persecución.

El abuso de los sistemas de información puede generar consecuencias nefastas. La perversa utilización de la información sensible de los ciudadanos colisiona con las garantías constitucionales propias de un Estado de derecho, porque información implica poder y éste aumenta la capacidad de control sobre los individuos, los que, cada vez más, se encuentran restringidos en su libertad y autonomía. Las empresas Infor.net, TransUnion, CrediRef es un ejemplo palmario de vulneración de derechos de los ciudadanos, como la intimidad y la libre determinación de las personas.

“La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico (por los intereses en juego), constituyéndose en un bien sustrato del tráfico jurídico, adquiriendo eminente relevancia jurídico-penal por ser posible objeto de conductas delictivas (hacking, cracking, fraude informático, espionaje y sabotaje informático, Etc.), que integran la delincuencia denominada de cuello blanco (pero no estrictamente económica) y por ser instrumento de facilitación, aseguramiento y calificación de los ilícitos tradicionales (casi todos los delitos, salvo aquellos que requieren una intervención físicamente directa y personal del autor como el abuso sexual con acceso carnal, son susceptibles de ser cometidos mediante el uso de sistemas de tratamiento, almacenamiento y flujo de la información, lo cual no implica que se traten de delitos informáticos).

Consecuentemente, adelantando la respectiva toma de postura, consideramos que el bien jurídico tutelado en los delitos informáticos, es la información en sí misma, en toda su amplitud (titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad), sin perjuicio de que con su ataque, subsidiariamente y tratándose de un interés colectivo, afecte otros bienes jurídicos como la intimidad o la propiedad²⁰.

Si aprueban una nueva ley se deberá tener presente que el derecho penal es la última ratio del orden normativo, el último instrumento de control social, a disposición del Estado para la prevención de la criminalidad, contrabando de información y venta, por lo que su utilización debe limitarse a la intervención necesaria, mínima, para preservar la convivencia humana en el país.

El sistema de reacciones penales, por su poder represivo, debe estar necesariamente precedido por medidas de políticas económicas y sociales que, en lo posible, operen preventivamente sobre las causas de la criminalidad. En su caso, debe intentarse la protección del bien jurídico con remedios jurídicos y penales. Consecuentemente, se desprende que no todos los bienes jurídicos deben ser protegidos penalmente y que sólo se incriminan las lesiones más graves al bien jurídico (el derecho penal es fragmentario).

Sentado lo expuesto, se debe dejar en claro cuál es el bien jurídico protegido en los delitos informáticos.

En el entendido que la norma penal tiene una función protectora de bienes jurídicos y que para cumplir dicha función, eleva a la categoría de delito, por medio de la tipificación legal, aquellos comportamientos que más gravemente los lesionan o ponen en peligro. “En cuanto al bien jurídico en sí, se comparten los alcances de las concepciones trascendentes, en cuanto a que la realidad social es la que le otorga su contenido. Los bienes jurídicos son intereses vitales del individuo o la comunidad, el

²⁰ **ibid**

orden no puede crearlo, lo crea la vida, pero la protección del derecho eleva el interés vital al bien jurídico.

En definitiva, si bien es cierto que el legislador recepta los intereses vitales colectivos como bien jurídico al otorgarles especial protección jurídico penal y que, en ese contexto, verdaderamente son compartidos por la mayoría de los ciudadanos, no lo es menos que, determinadas conductas meramente desviadas, respondiendo a diversos intereses, pueden etiquetarse también como delitos, sin que, esencialmente, ostenten dicho carácter. Ello no significa, en modo alguno, que no deban ser protegidos los intereses involucrados, sino que la respuesta debe ser hallada mediante algún otro mecanismo de control social y no en el que representa el poder punitivo del Estado^{.²¹}

“En definitiva y tal como se adelantó, atendiendo a las características de esta nueva era y sus implicancias ya descritas, se entiende que el bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, Etc.)^{.²²}

“Se dice, acorde con la postura sustentada en torno al bien jurídico tutelado en los delitos informáticos, con las tradicionales distinciones doctrinales de estas conductas ilícitas en delitos informáticos de carácter económico y aquellos que atentan contra la privacidad. En primer lugar, porque toda la información –aún la privada– posee un valor apreciable económicamente y en segundo, porque los intereses vulnerados superan el marco meramente patrimonial, verificándose un verdadero carácter pluriofensivo de las conductas delictivas, por implicar afectación de cuestiones que atañen a la seguridad y a la confianza en el correcto funcionamiento de los sistemas informáticos que repercuten en la vida social colectiva. Por otra parte, tal reduccionismo haría

²¹ <http://delitosinformaticos.com/trabajos/hacking.pdf>

²² **Ibid**

innecesaria la creación de la categoría de los delitos informáticos, puesto que no serían más que delitos contra la propiedad, o bien, contra la intimidad o privacidad".²³

Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, pero tienen como objeto del injusto la información en sí misma, la cual, como se expresó, posee múltiples características que trascienden lo meramente económico. A continuación se señala cuáles son las conductas lesivas a la información, según el Consejo de Europa y el XV Congreso Internacional de Derecho, entre otras:

1. Fraude en el campo de la informática.
2. Falsificación en materia informática.
3. Sabotaje informático y daños a datos computarizados o programas informáticos.
4. Acceso no autorizado.
5. Intercepción sin autorización.
6. Reproducción no autorizada de un programa informático protegido.
7. Espionaje informático.
8. Uso no autorizado de una computadora.
9. Tráfico de claves informáticas obtenidas por medio ilícito.
10. Distribución de virus o programas delictivos.

Consecuentemente, se entiende por delitos informáticos aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcando otros intereses: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, contrabando de datos, Etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión

²³ **Ibid**

y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas.

CAPÍTULO III

3. Derecho de la privacidad

El derecho que todo guatemalteco tiene de nacer y de la misma forma en que nace libre físicamente, tiene la libertad de dar a conocer de sí mismo, a la sociedad lo que su voluntad le sugiera, pero con el desarrollo de la tecnología y la creciente demanda de información de nuestros días, esto parece ser imposible.

Esta consideración encuentra una explicación bipolar, ya que por un lado puede tratarse de la inseguridad que representa el almacenamiento, ensayo, recopilación o transmisión de datos, en las redes internas de las empresas públicas o privadas, así como de la misma red mundial, o bien, a pesar de la seguridad, debido al ingenio que poseen personas que por diversas razones se aplican en la manipulación de sistemas informáticos ajenos, ya sea por una u otra de las alternativas, la intimidad de las personas se ve conculcada.

Así pues en el presente apartado justificare la urgente e indispensable la creación de una norma respecto de la protección de los datos que se almacenan, investigan, recogen o transmiten por medios electrónicos.

Si bien la información es un elemento indispensable para la toma de decisiones y que toda persona nace con la garantía de acceso a las noticias y demás acontecimientos, también lo es que el hombre nace con la plena facultad de decidir con quien compartir sus ideas, sentimientos o hechos de su vida personal o simplemente reservarlos para sí mismo.

El derecho de disponer de los datos es de quien los ha tratado, se puede decir que si tal garantía es violada, se estaría en presencia de un atentado a las libertades individuales, violando así lo establecido en el Artículo 31 de la Constitución Política de la República de Guatemala.

Las libertades individuales son: “Las Facultades reconocidas al individuo en todo Estado de Derecho, para el desenvolvimiento de su personalidad”.²⁴

Sin duda los adelantos tecnológicos y el progreso ideológico han venido a facilitar la vida del hombre, pero, tales son las facilidades que ha brindado la tecnología, que se ha abusado de ella. La capacidad de almacenaje, la velocidad de consulta y de transmisión de información, de una computadora, da para quien cuente con una de ellas una especie de poder, económico, psicológico, social, y político.

Tanto el derecho a la información como el derecho a la intimidad, son derechos fundamentales en la vida del hombre de estos tiempos. No obstante, la distancia que guardan estos dos conceptos, se encuentran hoy en día, estrechamente vinculados, esto debido al mal sentido que se le ha dado al derecho de ser informado, pues abusando de este último, es como se transgrede el derecho de la intimidad.

El derecho a la información es una garantía individual de carácter social. Se puede afirmar que la información es el intercambio de ideas, la comunicación de acontecimientos, pensamientos, sentimientos, Etc. La comunicación de la información puede ser masiva o de puede ser comunicación interpersonal. El legislador se ocupó de adicionar esta garantía al lado de la de la libertad de expresión, por medio de las cuales el Estado se compromete a proteger el derecho de unos a manifestar las ideas o comunicar los hechos y de que otros se enteren de toda esa información.

El derecho a la información es una garantía constitucional, contenida en el Artículo 31 de la Constitución Política de la República de Guatemala, que establece: "... Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos..."

²⁴ De Pina Vara, Rafael, **Diccionario de derecho**, pág. 360.

El Estado garantiza, el derecho a la información, que en un principio estaba dirigido únicamente a fines electorales, lo que podemos corroborar con la siguiente tesis relativa a la interpretación del Artículo 31 de nuestra ley primaria.

La concepción respecto de la interpretación del Artículo 31, es que el derecho a la información es la facultad de cualquier persona de solicitar sin manifestar su motivo, la información que requiera y a recibirla de cualquier autoridad, también es el derecho a conocer la verdad, siempre que esta no atente contra la moral, el Derecho, el país o a terceros. De esto último se desprende que el Estado por un lado, garantiza en el 31 precepto constitucional la información y que esta sea veraz, completa y oportuna y por el otro lado protege la información personal o privada.

El derecho a la información comprende dos vertientes, a saber, el deber de informar y el derecho a ser informado.

El deber de informar. Esta vertiente comprende desde los actos la investigación, recopilación y demás actividades destinadas a la obtención de información hasta los de difusión de la información, es decir, es la parte garantizada por la constitución denominada libertad de expresión.

El derecho a ser informado. Es el derecho de los individuos a estar comunicados respecto de los sucesos públicos y en general de todo acontecimiento o idea que pueda afectar su vida personal o le pueda hacer cambiar su forma de pensar. Pues como se dijo la información dota de poder y permite realizar con mayor eficacia las relaciones sociales y laborales. Sopesando que una garantía constitucional no puede de ninguna manera quebrantar algún otro derecho.

La necesidad de esconder hechos, opiniones, pensamientos y sentimientos es imprescindible para todo ser humano. Todos tienen un espacio en sus mentes, sus documentos, inclusive en sus archivos secretos en sus computadoras, en el que guarda antecedentes que mantiene en secreto momentánea o permanentemente, tal espacio debe mantenerse en la calidad que se guarda en tanto el titular lo desee, por lo

tanto, el respeto a esa determinación no solo obedece a los valores éticos, sino que lo respalda el derecho. Como anteriormente se observó, el derecho a la intimidad se desprende de la interpretación del Artículo 31 de la Constitución, sin embargo la protección legal de la intimidad en Guatemala no existe.

Y lo establecido en el Decreto 57-2008 Ley de Acceso a la Información Pública, como única medida de seguridad para los datos personales o privados, esto es, para garantizar el derecho a la intimidad, resulta pobre, pues si bien existe una tesis que ampara este derecho, también es cierto que la mayoría de las personas la desconoce. Aunque el derecho a la intimidad es un derecho esto no ha sido suficiente, para nuestros legisladores, para dar fuerza legal a tal garantía. Empero, no solo el Artículo 31 le ha dado vida en nuestro país al derecho a la intimidad, pues en el año de 1966 la asamblea general de las Naciones Unidas adopto un Pacto de Derechos Civiles y Políticos, mismo que manifiesta en su Artículo 17 establece que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, su correspondencia ni ataques ilegales a su honra y reputación.”

Si se considera que la definición de la intimidad es la parte reservada o más particular de los pensamientos, afectos o asuntos interiores de una persona, familia colectividad, es fácil deducir que a esa información, sólo se tendrá acceso con la autorización de su titular (es), por el valor moral, social, político o de otro tipo que guarda determinada información.

Definitivamente el derecho a la intimidad se encuentra en conflicto con la cultura de información, específicamente y por lo que atañe a la presente investigación, con la información automatizada. Empero no con el derecho a estar informado, pues el derecho a la información no comprende los datos de una persona o empresa que no son susceptibles de publicar. Un claro ejemplo es que la Corte Suprema Argentina sostuvo que el derecho a la intimidad contenido en el Artículo 19 de su Constitución ampara “la autonomía individual integrada por sentimientos, hábitos, costumbres, relaciones familiares, posición económica, creencias religiosas, salud mental y física y todos los hechos y datos que integran el estilo de vida de una persona que la

comunidad considera reservadas al individuo y cuyo conocimiento o divulgación significa un peligro para la intimidad”.²⁵

3.1. Concepto

“El derecho a la intimidad es la facultad que le reconoce el Estado al hombre de mantener reservada la información que considere no comunicable. Entonces el hombre decide cuales son los datos que debe limitar a su saber y el Derecho es el que se encarga mediante sus leyes de evitar la intromisión de terceros a dicha información”.²⁶

Antes de describir el hábeas data se conocerá un poco de la figura en la que se basa esta institución, a saber, el habeas corpus. Es una figura jurídica que encuentra su origen en el derecho inglés, el habeas corpus tiene como finalidad la libertad personal de los individuos. Esta institución se debe a la reacción de los sujetos pasivos de abusos a su libertad por parte de personas que no eran autoridad jurídica, es decir, por parte de la corona y otros. Los monarcas eran arbitrarios y ordenaban privación de la libertad y estas se llevaban a cabo sin orden judicial alguna.

El habeas corpus ha tenido un gran desarrollo en países como Inglaterra y Estados Unidos aunque consta en un cuerpo legal muy antiguo (1679 en Inglaterra), tiene su fundamento en la jurisprudencia y costumbre de estos países y tiene una gran fuerza jurídica por el sistema de derecho anglosajón, un derecho consuetudinario.

En pocas palabras se puede definir al habeas corpus como una institución jurídica destinada a proteger la libertad personal de las personas. De la misma manera que se nace con la libertad física, se tiene la libertad de disponer libremente, de disponer sobre la información que le pertenece, como los sentimientos, las ideas y en general todo lo que la imaginación y cultura permita crear.

²⁵ Palazzi, Pablo Andrés, **El Hábeas Data en el derecho argentino**, pág. 10.

²⁶ Ekmekdjian, Miguel Angel y Pizzolo, Calogero. **Habeas**, pág. 56.

El hábeas data puede ser concebido como un derecho que protege de las personas que se dedican a acceder a registros o bancos de datos y de esta forma conocer los datos personales que han sido almacenados y darles diferentes utilidades, comerciales, políticos y personales principalmente.

El hábeas data garantiza la vida privada de una persona, que nadie viole las áreas de actividad de una persona no destinadas a ser difundidas, sin su consentimiento. También ampara la intimidad ante las autoridades, las que sólo podrán acceder a la información privada cuando esta ponga en peligro la seguridad de la nación o exista el peligro de un bien jurídico superior si determinada información no es revelada.

Al realizar un estudio acerca de esta figura no se intenta sólo justificar y fomentar el estudio del derecho a la intimidad, sino se quiere informar acerca del manejo de la información por parte de personas públicas y privadas sin previa autorización de los titulares de tales datos. La manipulación de datos sin permiso, se ha vuelto una práctica normal en la sociedad guatemalteca, se piensa que esto se debe a la omisión de cuidar la intimidad o lo que es lo mismo, no se ha puesto barreras limitativas a las personas que se encargan de manejar los datos de los guatemaltecos.

El principal factor de creación del hábeas data se considera que ha sido el cambio radical que ha impuesto en las vidas de las personas la informática y demás herramientas tecnológicas de punta, esta es la postura de estudio que se adoptará en este análisis del hábeas data. Cabe hacer la aclaración de que el Hábeas Data no sólo protege la intimidad del hombre, sino también la verdad e identidad de los datos del individuo que han sido registrados.

De lo anteriormente expuesto resulta que "el hábeas data protege un **complejo de derechos personalísimos**, que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad".²⁷ Sin embargo, el sentido que se quiere dar al Hábeas Data en la presente investigación es que su propósito se

²⁷ *Ibid*, pág. 56.

dirige a evitar las lesiones morales que atentan contra la intimidad de las personas. Y en este concepto han coincidido la mayoría de los autores que estudian el Derecho de la Informática.

3.2. Clases

Existe información que por su importancia debe ser publicada a la sociedad por los medios que mayor audiencia tengan. Empero, no todos los datos deben ser publicados, esto en razón de que la publicación de algunos datos podría atacar el honor, los sentimientos o las creencias de algunas personas. En atención a lo anterior se considera que la información procesable se divide en: datos reservados y datos públicos.

“1. Se considera como datos reservados la información que también se conoce como sensible y que comprende todas aquellas situaciones íntimas de las personas, como lo es la religión, las ideas socio-político y económicas, la situación económica personal, las preferencias sexuales, la raza y demás condiciones que atañen únicamente al individuo y que de reservárselas no perjudica a nadie, no obstante, de ser revelados o publicados podrían ocasionar un perjuicio.

Entre los datos sensibles que de ser difundidos sin consentimiento y que por obvias razones vulnerarían el derecho a la intimidad, se consideran los siguientes:

- La preferencia sexual de una persona.
- La religión que profesa una persona.
- El password o clave del e-mail de una persona.
- La dirección o número telefónico de una persona.
- Entre otras.

2. Los datos públicos son aquellos que importan a toda la sociedad y que se publican cumpliendo con el derecho a ser informado. Esto es que, el Estado está obligado

a mantener a sus habitantes informados de los hechos que en el país acontece con las reservas pertinentes y por lo tanto al publicarse provoca un beneficio para la sociedad.

Algunos de los datos públicos se consideraron los siguientes:

- Los resultados de las jornadas electorales.
- El presupuesto nacional.
- Los accidentes y crímenes.
- Las ofertas de trabajo.
- Entre otros".²⁸

Cabe señalar que un dato por insignificante que parezca puede llegar a provocar un daño irreparable, por lo que antes de la utilización de un dato sensible, por intrascendente que parezca, es indispensable solicitar el consentimiento del titular.

Como se dijo con antelación la definición el Hábeas Data obedece al reconocimiento de que es el individuo a quien pertenecen los datos quien debe ejercer el control de los mismos.

Empero, no es de sorprenderse el hecho de que la información considerada de carácter personal, pase de las manos de una empresa privada (como Infor.net, Transunion, Crediref, Etc.) a las de un Banco, a las de una empresa que ofrece sus productos o servicios, a las de un partido político o a las de una empresa que vende vía telefónica, todo esto sin que se tenga el conocimiento y aún más grave sin que consintamos tal tráfico de nuestros datos.

A ninguna persona se le consulta respecto de la inclusión de su información a determinada base de datos, simplemente le solicitan su información, para realizar algún trámite, principalmente en las entidades públicas. Generalmente no existe en los

²⁸ http://www.robertexto.com/archivo13/derintim_derinfo.htm

formatos que se llenan con información personal, una leyenda que consulte si la información puede ser anexada a un archivo (tradicional o electrónico), o por lo menos una leyenda que avise que la información será incluida en una base de datos. Considerando la inexistencia de notas como las que anteriormente se mencionaron, cuanto más existirán las que avisen que la información será compartida con una serie de empresas públicas o privadas o inclusive con personas físicas.

De esta manera es como los datos de millones de personas se encuentran registrados en bases de datos de personas y empresas que en ocasiones ni siquiera se conoce su existencia y que tales datos están disponibles para ser utilizados en el momento que esas personas consideren pertinente. De cualquier forma vivimos una situación de control opresivo de nuestra información y nuestros datos pueden ser utilizados sin que nos consulten y para los fines que terceros desean.

“Los datos suelen ser fáciles de obtener pues las empresas para la realización de cualquier trámite la solicitan y las personas sin cuestión alguna la proporcionan. No obstante, esta última no es la única forma de obtener información y en nuestro país no alarmaría a nadie la forma ilegal de obtener estos datos, esto alude al contrabando informático”.²⁹

“El mercado negro de bases de datos es la explicación que a todas luces se pueden encontrar, respecto de las cuestiones que muchas personas se hacen al recibir propaganda comercial y política generalmente. Sin embargo, las personas que reciben esta publicidad no se tornan ofendidas respecto a la disposición de sus datos sin su permiso, debido a que las campañas comerciales o políticas logran en el público un efecto psicológico, haciendo pensar a los receptores que son personas importantes para las grandes empresas o que son amigos de los políticos”.³⁰

“Otra vía de obtención es el alquiler de las bases, esta última también es ilegal. No se quiere hacer conjeturas, sin embargo lo evidente hace pensar que el tráfico ilegal de

²⁹ Beltramone, Guillermo. Zabale, Ezequiel, *El derecho en la era digital*, págs. 60-61.

³⁰ *Ibid*

información o la venta o alquiler se realiza generalmente del sector público al privado, esto responde a la completa información que el estado tiene de sus ciudadanos, esto último en el campo político y comercial que es lo más común, sin embargo, en cuestiones más confidenciales los bancos cuentan con información más detallada, se habla de datos de los cuales se puede deducir la forma de vida de una persona. Simplemente al hurgar en las operaciones de crédito realizadas por una persona podemos saber los lugares que frecuenta, el monto de dinero del que dispone diariamente, los productos que consume y los servicios que contrata, información que puede ser muy útil para las empresas inclusive hasta para los delincuentes, secuestradores y narcotraficantes.

Reiteradamente se debe asegurar que la disposición de los datos corresponde a quien la información pertenece, entonces el titular de la información para defender esa facultad de dar o no a conocer tales datos tiene ciertos derechos y entre todos esos nombraremos los siguientes:

- Acceso a los datos propios. Esta es la facultad que tiene el individuo de saber acerca de sus datos registrados en una base de datos o archivos y la utilización que se les puede dar. De este derecho prácticamente se desprenden los demás respecto de la titularidad de la información frente a la administración de la misma.
- Corrección y actualización de la información. Al tener el individuo el derecho de acceder a su información, también tiene el derecho de rectificar la veracidad de los datos y en su caso exigir la corrección, así como la actualización de los mismos.

La confidencialidad y exclusión en algunas bases de datos se registran datos de los que hemos clasificado como sensibles o información reservada. Tratándose de este tipo de registros el titular tiene todo el derecho de exigir al administrador de los comunicados la más estricta confidencialidad en relación con sus datos y en caso de conculcar esta facultad, el titular no tiene el poder jurídico suficiente para exigir la exclusión de su información de la base de datos o archivo respectivo,

independientemente de la acción judicial que tendrá por los perjuicios que le cause la revelación de su información sensible“.³¹

Por otro lado los operadores de los datos también tienen prerrogativas, pero todas ellas se reducen al derecho a ser informado, sin embargo este derecho está limitado a la voluntad del titular y a los derechos anteriormente señalados, por lo que el abuso de la información no tiene justificación alguna.

“La palabra intimidad, que viene del latín íntimus, superlativo de interior, designa cierto ámbito que se abre en lo que ya es interior. Es un lenguaje simbólico para dar a entender la dimensión propiamente espiritual del alma humana, que va más allá de la vida puramente biológica. A ésta la llamamos simplemente interioridad, para significar que la vida de un animal o planta es aquello que se le queda dentro, resistiendo a los cambios espaciotemporales sin disolverse ni convertirse en otra cosa. Y esto sólo es posible mediante el principio inmaterial que llamamos alma, o sencillamente vida. En el hombre sin embargo la interioridad es particularmente desarrollada y compleja debido a su autoconciencia. Para referirnos a tal complejidad solemos hablar de lo psicológico, ya que este es el objeto de la psicología y la psiquiatría. Pues bien, más allá de esta interioridad psicológica la vida humana presenta una dimensión única, que es inaccesible para la ciencia empírico-positiva porque no es un grado más de interioridad, sino un nuevo orden: el espiritual. En virtud del espíritu el hombre sabe y dispone de sí y es capaz de autoposeerse y autodestinarse; en una palabra, puede asumir la verdad última de su ser y decidir conforme a ella. La intimidad consiste precisamente en el ejercicio de esta libertad radical por la cual el hombre se hace fiel a sí mismo, al tiempo que se descubre inagotable, inabarcable, irreductible a las cosas“.³²

“La intimidad crea una distancia irreductible entre lo que se es y lo que se aparenta pues, a diferencia del animal, el hombre nunca está completamente dado. Esta inadecuación entre ser y aparecer, entre dentro y fuera, es el fundamento antropológico del pudor, el arreglo, el vestido, la elegancia. Paradójicamente tal distancia exige que el

³¹ **ibid**

³² http://www.darfruto.com/6_intimidad_privacidad.htm

hombre tenga que actuar si quiere ser auténtico, que deba interpretar el papel de sí mismo, hacer de sí. Ahora bien, no vale cualquier papel: tiene que ser aquel que la persona deduce de su propia intimidad mediante tres acciones simultáneas: a) Tomarse, adueñarse de sí mediante las virtudes y el temple moral; b) Confrontarse con los demás mediante el diálogo sincero; c) Inventarse el personaje que le cuadra en función de la escena social, eligiendo en todo momento la mejor versión de sí mismo: en esta autoelección estriba, precisamente, la elegancia, que proviene de elegir.

En la medida en que el hombre es consciente de la expresividad constitutiva de su cuerpo, que le manifiesta y le compromete incesantemente, en esa misma medida el cuerpo posee intimidad. Ésta se da, por tanto, según grados, de acuerdo a la madurez y la cultura. Un bebé, por ejemplo, no se puede decir que tenga intimidad corporal, aunque sin duda tiende naturalmente a desarrollarla.

Apenas la intimidad comienza a interpretarse socialmente en términos de identidad, en ese momento aflora la conciencia de la condición sexuada, que sitúa al individuo en el sistema sponsal. A partir de ahí la intimidad corporal se despliega gracias al lenguaje de la pureza de corazón, que se resume en el axioma: guardarse para darse. La intimidad adquiere entonces los infinitos matices expresivos de la complementariedad, que es como la voz con que el hombre percibe su vocación al don de sí amoroso.

Intimidad y comunidad no se contraponen, al contrario, la primera se realiza en la segunda; la intimidad sana aflora naturalmente en el diálogo, y cuando no lo logra se enrarece y se atrofia. La mentalidad dominante hoy, por el contrario, entiende la intimidad en términos de privacidad individualista, es decir confunde la intimidad con sus condiciones externas y su manifestación social. A ello hay que objetar que el concepto de privacidad pertenece a las cosas, no a las personas. Se llama privado al objeto que es poseído en exclusividad: la casa, el vestido, el utensilio, Etc., pero nunca a una persona o a una dimensión intrínseca de ella, como es su sexualidad. En este sentido caben dos extremos, éticamente erróneos:

- a) Supeditar la intimidad a la privacidad mediante un pudor excesivamente rígido. Con ello se pretende proteger la intimidad pero a costa de empobrecerla. Es el caso, por ejemplo, del burka usado por algunas mujeres musulmanas. Cuando esto ocurre el equilibrio de la complementariedad se altera en perjuicio de la mujer, que se convierte en posesión privada del varón.
- b) El otro modo de cosificar la intimidad, aún más grave y extendido, consiste en interpretarla como uso privado de la sexualidad, es decir, como si la simple privacidad convirtiera la sexualidad en intimidad. En esta actitud late la mentalidad utilitarista y hedonista, que se manifiesta en mil formas de conducta burda o frívola juzgadas, no obstante, como sociológicamente decentes³³.

3.3. Diferenciar privacidad e intimidad

Desde el punto de vista conceptual, en todas las legislaciones se dice de intimidad y privacidad como un solo concepto integrado. La privacidad se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por si misma puede no ser relevante, pero que analizada en un contexto concreto puede conducir a la construcción de un perfil fiable del individuo.

En Latinoamérica se ha desarrollado ampliamente el hábeas data. En la actualidad, no hay legislación que lo regule expresamente. En cuanto a la doctrina comparada, se encuentra unanimidad en que el hábeas data es una acción de carácter judicial, pero hay desacuerdo en cuanto a los derechos que tutela; una parte sostiene que el hábeas data es un mecanismo que protege el espacio íntimo de las personas en cuanto a los datos almacenados en computadoras y la otra, sostiene que el hábeas data protege el derecho a la información y tutela la identidad del individuo frente a la sociedad.

Cuando se dice de la protección de datos como derecho fundamental se tiende a hablar de los términos intimidad y privacidad indistintamente. Sin embargo, estos dos

³³ **Ibid**

términos tienen un alcance distinto que es necesario conocer para saber dónde empieza y termina el derecho a la intimidad, a la privacidad y a la protección de datos de carácter personal.

De igual forma, ubicamos a los derechos a la privacidad e intimidad en el cuadro de una sociedad abierta o libre, democrática y de la información o conocimiento como parte del desarrollo de la identidad personal y del libre desenvolvimiento de la personalidad al que tiene derecho toda persona conforme a su dignidad humana. Como señala Eusebio Fernández el concepto de dignidad humana gira en torno a “que cada uno de los seres humanos tiene un valor moral especial, que ha de ser reconocido y garantizado por las leyes y que significa, al mismo tiempo, el derecho a tener unos derechos básicos e inviolables”

El alcance de los derechos a la privacidad e intimidad y su colisión con otros derechos constitucionales y con algunos valores morales son cuestiones filosófico-jurídicas de gran relevancia que interesa debatir y no se pueden soslayar en una sociedad democrática y de la información.

Guatemala está en presencia de una sociedad basada fuertemente en imágenes, especialmente de los individuos, donde la información privada, personal, es fundamental en la construcción de perfiles. En efecto, como afirma Sartori, en su libro *Homo videns: La sociedad teledirigida*, “la premisa común sobre la que se basa de principio a fin es que el primado del ver, el primado de la imagen, empobrece el conocer y del mismo modo debilita nuestra capacidad de gestionar la vida en sociedad...”³⁴

En efecto, el derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra manera, describir intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información, o la relativa a la vida sexual, cuya difusión puede

³⁴ Sartori, Giovanni, *Homo videns: La sociedad teledirigida*, pág. 161.

producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionarían un individuo de manera libre y consciente.

La privacidad, sin embargo, es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo que permita su caracterización e identificación.

Existe un elemento que es común tanto en el concepto de intimidad como en el de privacidad: el tratamiento de la información personal. La información es, entonces, el elemento fundamental, la materia de la que están formadas privacidad e intimidad, en la cual ambas son dependientes.

Por lo anterior, se puede definir a la intimidad como "el derecho del individuo a decidir por sí mismo en qué medida desea compartir con otros su pensamiento y sentimientos, así como hechos de su vida personal y su entorno"³⁵, definición que se puede complementar con el pensamiento de Alan Westin en su libro *Privacy and Freedom* al decir que "la esencia de la privacidad es el derecho del individuo a ejercer el control de aquella información de sí mismo que desee compartir con otros, de la cantidad que de la misma facilite a otros, del momento en que desee hacerlo."³⁶

Por consiguiente, la cuestión a determinar es qué datos personales son privados y qué datos personales son públicos, ya que sí es posible comercializar la información de procesos y notificaciones judiciales siempre y cuando éstos datos personales tengan carácter de datos públicos y en el caso que tengan carácter privado será necesario contar con la autorización o consentimiento previo para su divulgación.

En concordancia, con la doctrina jurídico-informática se entiende por datos públicos, "aquellos datos personales que son conocidos por un número cuantioso de personas

³⁵ Carrascosa, Valentín, **Derecho a la intimidad e informática**, en *revista informática y derecho*, pág. 11.

³⁶ **Ibid.**

sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato, ni, por la calidad del dato, pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites de respeto y de convivencia cívicos, teniendo en cuenta además que la conciencia social es favorable a su publicidad, siendo frecuente su difusión como si no se tratara de datos personales"³⁷. En este sentido serán públicos, por ejemplo los datos identificativos del nombre, apellidos, edad o profesión de una persona que, aunque no está obligado a darlos a cualquiera que se los demandare, no puede impedir que una vez conocidos sean difundidos.

Por otra parte, serán privados, "aquellos datos personales que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos, o ponerlos en conocimiento de terceros, siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular"³⁸. Mientras en Guatemala no se norme o regule la protección de datos considerados de carácter personal no será posible comercializar libremente la información de procesos y notificaciones judiciales que tienen el carácter de datos públicos y cuando tengan el carácter de datos privados, se requerirá previo consentimiento. Además deberá resguardarse la integridad y veracidad de los datos.

En algunos países, Brasil, Argentina y Colombia los datos por su naturaleza están divididos de la siguiente forma de acuerdo a su legislación:

- a) Datos sensibles; como son el de raza, ideología, estado de salud, creencias, religión.
- b) Datos secretos; como son el secreto profesional, secreto comercial, secreto bancario, secreto de confesión.
- c) Datos reservados; son aquellos que el titular no está obligado a proporcionar para que sean conocidos por terceros, como son: filiación (hijo matrimonial, extramatrimonial, adoptado), delitos contra el honor (difamación, calumnia, injuria), libertad sexual (violación), adulterio, aborto, Etc.

³⁷ Davara Rodriguez, Miguel Ángel, **Manual de derecho informático**, pág. 51.

³⁸ **Ibid.**

- d) Datos privados; los que el titular debe proporcionar periódicamente a la autoridad para fines específicamente señalados, por ejemplo los datos contenidos en una Declaración Jurada del Impuesto a la Renta, sólo deben ser utilizados para los fines que específicamente fueron dados, no para fines distintos“.³⁹

3.4. Protección de los datos personales

Es indudable que con el correr de los años la posibilidad de disponer información sobre las personas ha ido paulatinamente en aumento. Si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo informático y globalizado de hoy, surge con pocos cuestionamientos el derecho de las personas a protegerse frente a la intromisión de los demás.

Un régimen de protección de los datos personales permite que los ciudadanos ejerzan su legítimo poder de disposición y control sobre los datos de carácter personal referidos a su persona que se encuentran registrados en bases de datos de titularidad de terceros.

A tal fin, la legislación debe facultar a los ciudadanos a decidir cuáles de esos datos quieren proporcionar a terceros, sea el Estado o un particular, o qué datos pueden esos terceros recabar, permitiendo asimismo que sepan quién posee sus datos personales y para qué, pudiendo inclusive oponerse a esa posesión o uso.

Estos poderes de disposición y control sobre los datos personales, se concretan jurídicamente en la facultad de consentir recoger, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento

³⁹ *Ibid.*

quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

La Ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

En el derecho anglosajón se denomina *privacy* y que se ha castellanizado como *privacidad*. Lo que se busca es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia pero que, al unirse con otros, pueden configurar un perfil determinado de las personas. Ante dicha posibilidad surge el derecho de sus titulares a exigir que los datos permanezcan en el ámbito de su *privacidad*.

En consecuencia, puede definirse al concepto de protección de datos como el amparo debido a los ciudadanos contra la posible utilización de sus datos personales por terceros, en forma no autorizada, para confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad, o como la protección de los derechos fundamentales y libertades de los ciudadanos contra una singular forma de agresión: el almacenamiento de datos personales y su posterior cesión.

Lo anterior ocurre, pese a estar regulado por la Constitución Política de la República de Guatemala Artículo 31 “Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos” y Artículo 44 “Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana...”

En el Código Penal en el Artículo 274 “D” “...Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas” y desde el 2008 por la Ley de Acceso a la Información Pública Artículos 9 numeral 2 “...Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza...” y Artículo 64 “Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales y el comiso de los objetos instrumentos del delito.

La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles”.

3.5. El derecho de privacidad del individuo

La propuesta de crear una Ley de Protección de Datos Personales debe exigir que todo aquel que efectúe operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relevamiento, evaluación, bloqueo, destrucción, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, interconexiones o transferencias, debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento de este tipo de información.

Deben existir normas que al referirse a la seguridad de los datos señalen que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Se debe prohibir registrar datos personales en archivos, registros o bancos de datos.

Debe existir un departamento de protección de datos personales y que sea dicho organismo el encargado de dictar las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros, bases y bancos de datos públicos y privados.

Como se ha señalado, la necesidad de protección de la vida privada no es de reciente desarrollo, sino que se constituye en principal elemento de la libertad individual, y como tal es reconocida mundialmente. Sin embargo, el fenómeno del comercio electrónico acentúa la fragilidad de la privacidad individual y crea nuevos y grandes retos en materia de su protección.

La noción de intimidad o privacidad está ligada al nacimiento del llamado Estado Liberal, y se desarrolla por primera vez con el llamado constitucionalismo inglés. En esta rama del Derecho Anglosajón se dieron las primeras discusiones sobre el tema de la libertad y la autonomía.

Lo que hoy en día se conoce como derecho a la privacidad tiene sus orígenes en los Estados Unidos, donde por primera vez es tratado como categoría independiente de derechos. A finales del siglo XIX, en un artículo titulado *The Right for Privacy*, Samuel D. Warren y Louis Brandeis, se basaron en los principios del common law para intentar establecer un límite jurídico con fundamento en el cual se pudieran prohibir las intromisiones de la prensa en la vida privada y doméstica. En su introducción, Warren y Brandeis exponen que:

“...en un principio, la ley aportó solución sólo a la interferencia física con la vida y la propiedad, a las transgresiones vi et armis. Entonces, el derecho a la vida servía sólo para proteger al sujeto de lesiones en sus distintas formas; tener libertad significaba vivir libre de restricciones reales; y el derecho a la propiedad aseguraba al individuo el derecho sobre sus tierras y ganado. Posteriormente, surgió el reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos y su intelecto. Gradualmente, el espectro de estos derechos jurídicos se amplió, y ahora el derecho a la vida se ha convertido en el derecho a disfrutar la vida, el derecho a ser dejado en paz. Ahora, el derecho a la libertad permite al individuo el ejercicio de extensos privilegios civiles; y el término propiedad ha crecido para abarcar todas las formas de posesión, tanto intangible como tangible”.⁴⁰

En su artículo, Warren y Brandeis reflejan el problema del derecho a la privacidad, que ya antes de 1890 se manifestaba en la sociedad estadounidense y lo cual generaba bloqueo para las personas que se veían afectadas por este derecho.

“Recientemente han surgido inventos y métodos de negocios que llaman la atención al próximo paso que debe darse en materia de protección al individuo, y para la preservación de lo que el juez Cooley llama el derecho ‘a ser dejado en paz’. Las fotografías instantáneas y la empresa periodística han invadido los sagrados precintos de la vida privada y doméstica, y una gran cantidad de dispositivos mecánicos amenaza con hacer cierta la predicción de que ‘lo que se murmura en los armarios será proclamado en los techos de las casas’. Durante años ha existido el presentimiento de que la ley debe aportar algún remedio a la circulación no autorizada de fotografías de personas privadas; y la maldad de la invasión de la privacidad por los periódicos se viene sintiendo desde hace mucho, y fue recientemente discutida por un gran escritor. Los hechos alegados en un caso notorio, del cual conoció un tribunal de primera instancia en Nueva York hace algunos meses, incluyen directamente la consideración del derecho a circular retratos, y pone en evidencia que nuestras cortes deberán muy

⁴⁰ Samuel D. Warren y Louis Brandeis, **The Right to Privacy**, Harvard Law Review, No. 5. Vol. IV, pág. 442.

pronto tendrán que decidir casos en los que deban considerar si la ley debe reconocer y proteger el derecho a la privacidad en torno a éste y otros aspectos.”⁴¹

En Guatemala existe una necesidad de crear leyes que sobrevivan al paso del tiempo, aspecto interesante puesto que demuestra que a principios del siglo pasado ya existía la conciencia del carácter cambiante de las realidades, y de la necesidad de crear normas que se adaptaran a tales cambios. Las leyes deben ser capaces de una aplicación más amplia que la requerida por la transgresión que causó su redacción, la aplicación de una Constitución no es suficiente para contemplar lo que ha sido o lo que es, sino lo que puede ser. Las normas que garantizan el derecho a la protección de los individuos contra abusos de poder específicos deben tener una capacidad similar para adaptarse a un mundo cambiante.

Con relación a la protección brindada por la Constitución estadounidense al derecho a la privacidad, Brandeis escribió que los redactores de la Constitución se dieron a la tarea de asegurar la existencia de condiciones favorables a la consecución del bien común, y reconocieron el significado de la naturaleza espiritual del hombre. En este sentido, Brandeis explicó en su voto que “el derecho a la privacidad en los Estados Unidos está protegido constitucionalmente, específicamente por la Cuarta y Quinta Enmiendas. Según su opinión:”⁴²

“Ellos quisieron proteger a los americanos en sus creencias, sus pensamientos, sus emociones y sus sensaciones. Ellos confirieron a los ciudadanos el derecho, oponible al gobierno, de ser dejados en paz, el más amplio de los derechos y el más valorado por los hombres civilizados. Para proteger ese derecho, cualquier invasión del gobierno a la privacidad del individuo que no esté justificada debe ser considerada como una violación de la Cuarta Enmienda, sin importar qué medios se hayan empleado. Asimismo, el uso de pruebas obtenidas mediante tales invasiones como evidencia en un juicio debe ser considerado una violación de la Quinta Enmienda.”⁴³

⁴¹ *Ibid*, pág. 442.

⁴² *Ibid*, pág. 443.

⁴³ *Ibid*, pág. 443.

Brandeis se basó en la Cuarta y Quinta Enmiendas a la Constitución de los Estados Unidos para delimitar lo que es el derecho a la privacidad, y así lo instituyó este derecho como una institución jurídica que ha sido desarrollada en el mundo entero.

En Europa, el origen del derecho a la privacidad está vinculado a los derechos de la personalidad propios del Derecho Civil, y se consideraba este derecho como un medio para proteger al individuo en su forma de ser, excluyendo del conocimiento ajeno todo cuanto se refiere a la persona misma. En la Resolución N° 428 del 23 de enero de 1970, la Asamblea Consultiva del Consejo de Europa señala que:

“El derecho al respeto de la vida privada consiste, esencialmente, en poder realizar la vida como uno entiende, con un mínimo de injerencias. Conciernen a la vida privada, vida familiar y la vida del hogar, la integridad física y moral, el honor y la reputación, el hecho de no ser presentado bajo una falsa imagen, la no divulgación de hechos banales y bochornosos, la publicación sin autorización de fotografías privadas, la protección contra el espionaje y las indiscreciones injustificables o inadmisibles, la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular (...) el hecho de que un individuo ocupe un puesto destacado en la actualidad no le priva del derecho al respeto de su vida privada.”

La Resolución N° 428 antes citada revela el nivel de especificidad de las disposiciones que con respecto al derecho de privacidad se han redactado en Europa. Tal especificidad se debe, a la gran preocupación existente en los países europeos por el respeto al derecho a la privacidad, lo cual se evidencia aún más en legislación posterior, tanto del Derecho Comunitario Europeo como del Derecho Interno de cada país. Por lo demás, la definición transcrita parece una conceptualización ideal de lo que es el derecho a la privacidad. Sin embargo, hoy en día el Derecho europeo se ha dirigido en ciertos casos hacia tendencias que permiten mayor acceso la información personal de cada individuo, tema que ha causado grandes controversias en el mundo jurídico y que constituye el problema fundamental.

Hoy en día la sociedad aprovecha estas diversas aplicaciones de la ciencia y la tecnología. El desarrollo tecnológico ha cruzado fronteras antes inalcanzables o impensables, trazando nuevos senderos para la exploración humana. El hombre contemporáneo ha desarrollado una relación casi simbiótica con las aplicaciones tecnológicas a su alcance. Sin duda alguna, el escenario cotidiano se ha enriquecido con múltiples beneficios, acarreando transformaciones sociales de gran trascendencia.

Sin embargo, este proceso no se integra por bondades exclusivamente, lleva implícitos peligros inobservados en muchas ocasiones. Por ello, el desarrollo tecnológico debe acometerse en forma armónica con el respeto a la dignidad humana, sin que ninguno de ellos se convierta en opresor del otro.

El uso de las tecnologías de la información implica el respeto al derecho a la privacidad y una participación interdisciplinaria para lograrlo. Para ello, es necesario conocer la operación de los sistemas de información y su involucramiento con la privacidad individual.

La ciencia, como actividad humana, puede ser concebida desde el momento cuando el hombre intenta encontrar una explicación lógica a los fenómenos ocurridos en su alrededor. Comienza con la simple observación y experimentación como medios de adquisición del conocimiento, para posteriormente darle un significado y organización. Posteriormente, transforma el conocimiento de una aprensión mental a una aplicación práctica. Iniciando así, la creación de la tecnología.

A lo largo de la historia, el hombre ha desarrollado la tecnología incrementando su eficiencia y complejidad conforme se acrecienta el conocimiento humano. Le ha dado innumerables aplicaciones en la vida diaria, determinando de esta forma el desarrollo de las sociedades y su transformación educativa y cultural. Las sociedades que han aprovechado las aplicaciones tecnológicas han podido alcanzar un mayor grado de desarrollo económico y social.

A principios del siglo XX, se dio una gran transformación social propiciada por dos factores: por un lado el veloz incremento del conocimiento humano y su aplicación práctica; y por el otro lado, la disposición de la sociedad para beneficiarse de los nuevos sistemas tecnológicos. El resultado es un valor apreciable, pero inmensurable, de la información; no obstante, se le asigna un valor económico.

Ahora la información es considerada apropiable, se convierte en una mercancía más y en un parámetro de medición. El valor de los bienes está directamente relacionado con la información requerida para su elaboración. Bajo este esquema, el trabajo intelectual es el motor de un negocio, y mejor retribuido respecto al trabajo físico.

El cuantioso cúmulo de información adquirida se convirtió en terreno fértil para las tecnologías de la información. Con ellas se proporciona un manejo ágil y eficaz de la información mediante bases de datos y estructuras de transmisión las cuales, combinadas integran un servicio de información.

La complejidad de estos servicios que pueden ir desde una conexión entre dos computadoras hasta la Internet. Así, la información puede compartirse y se facilita la actualización de la misma, pues al ser actualizada una sola base de datos, todos los usuarios del sistema obtendrán al mismo tiempo dicha actualización. También pueden asociarse unos datos con otros para producir nuevos datos informáticos. Este sistema de trabajo ha esculpido a la sociedad actual.

Cuando los datos manipulados en los servicios de información incluyen aspectos relacionados con el ámbito de la privacidad de los individuos, surge un conflicto entre dos derechos fundamentales: el derecho a la información y el derecho a la privacidad.

Los riesgos de violación de derechos y libertades fundamentales mediante el uso de las nuevas técnicas informáticas se hacen más evidentes en el caso de las llamadas informaciones sensibles (datos sobre creencias o convicciones religiosas, opiniones políticas, origen racial, hábitos sexuales, circunstancias penales y pertenencia a

sindicatos o partidos políticos, Etc.), que pueden dar lugar a conductas discriminatorias por parte de quienes tienen monopolios de información.

En suma, estos son los datos descriptivos de la privacidad humana relacionada a un nombre. Mediante el ordenamiento y sistematización de diversos datos de una persona por ejemplo: viajes realizados, uso de tarjeta de crédito, registros de compras, solicitudes de ingreso a clubes, Etc. se puede obtener un perfil de comportamiento que restringe la libertad de la persona, es el denominado inferential relational retrieval, del cual se deriva la autodeterminación informativa.

En Guatemala se estima que existen ocho empresas con sistemas de información y que ofrecen sus servicios al público, abriendo las puertas a la difusión o mal uso de las informaciones sensibles. Algunos servicios son proporcionados a través de redes privadas, otros usan la Internet, y algunos utilizan ambos canales. En este punto es donde surgen grandes preocupaciones, pues la Internet no pertenece a nadie y todos los usuarios de computadoras quieren aprovechar las capacidades de esta mega red.

Pero no se han establecido normas jurídicas destinadas a regular su funcionamiento; hasta el día de hoy la única normatividad al respecto está determinada por la autorregulación y las limitaciones de carácter técnico. Por todo ello, resulta indispensable establecer normas jurídicas que garanticen la protección al Derecho a la Privacidad en Guatemala.

Por no existir una norma específica que regule la protección de datos de carácter personal de la ciudadanía guatemalteca, sólo queda esperar la aprobación en definitiva de la iniciativa de ley de protección de datos personales, la cual se encuentra en el Congreso de la República de Guatemala con dictamen favorable de la comisión de economía, identificada con el registro número 4090 de fecha 20 de agosto de 2009.

CAPÍTULO IV

4. El Estado de Guatemala y el hábeas data

El hábeas data tiene entre sus antecedentes a la acción de hábeas corpus. El vocablo habeas proviene del latín habere, que significa téngase en su posesión y data, proviene del inglés que significa datos, definido por los diccionarios como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos. Por lo que hábeas data quiere decir téngase los registros, los datos.

En la doctrina comparada hay unanimidad en que la formulación hábeas data se origina parcialmente en el hábeas corpus, pero mucho se ha discutido con respecto a la significación de la palabra data.

“Con referencia a esta última existen dos vertientes, una según la cual data, es un acusativo neutro plural de datum, de la misma raíz que el verbo latino do, das, dedi, datum, dare, dar, ofrecer. Datum, singular de data, es empleado con el sentido de presentes, donativos, ofertas y no con el sentido de datos.

La vertiente contraria sostiene que la palabra data proviene del inglés, posición que encuentra como fundamento el hecho de haber sido utilizado en tal sentido por la Data Protection Act inglesa, la Data Lag sueca, la Federal Data Protection Act austríaca, y otras...“⁴⁴

Por tanto se puede colegir que el hábeas data es considerado como una posible acción judicial tendiente a permitir el acceso a los datos que se encuentran almacenados en registros, tanto públicos como privados, a los fines de controlar dicha información y, en

⁴⁴ Defensoría del Pueblo, 1998. Defensoria.com.ve.

caso de que dicha información sea falsa o discriminatoria, se podrá solicitar la supresión, rectificación, confidencialidad o actualización de ésta.

Los motivos del hábeas data, según la legislación, debieran permitir que sea dividido en dos etapas, el derecho al acceso y, posteriormente, el derecho a la supresión, rectificación o confidencialidad, en el supuesto de que sea falsa o errónea.

En cuanto al origen de esta acción, tenemos que las primeras constituciones en abordar el tema sobre la problemática de la explosión informática fueron las de España (1978) y Portugal (1976), aunque realmente dichas disposiciones no establecieron acciones jurisdiccionales especializadas en proteger y combatir los efectos negativos del fenómeno informático.

Es realmente a partir de los procesos constituyentes de los países latinoamericanos donde ha tenido mayor desarrollo esta institución, siendo en Brasil donde se puede localizar el origen de esta acción con este mismo nombre, en el Artículo 5, numeral LXXII, de la Constitución de 1988, que establece:

"Conceder el hábeas data: a. Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que conste en registro o en banco de datos de entidades gubernamentales o de carácter público. b. Para la rectificación de datos, cuando no se prefiera hacerlo por procesos reservados judicial o administrativo".

A partir de dicha disposición, comienza a incorporarse dentro de las diferentes Constituciones latinoamericanas la acción del hábeas data, ya sea con ese nombre o con uno diferente, o bien como un derecho. En este sentido, se tiene la Constitución Política de la República de Guatemala, Artículo 31 que lo reconoce como una garantía y no como un proceso autónomo.

El hábeas data, por tratarse de una institución relacionada con la informática y por consiguiente con la creación de archivos, registros y bases de datos, es menester establecer el objeto o la finalidad que se persigue con dicha institución. En un sentido

literal, el Hábeas Data parte de la idea inicial de la obtención de datos, pero es necesario aclarar cuáles datos son los que se pueden obtener, ya que se podría interpretar que sería con respecto a cualquier tipo de datos.

Es así como, los datos a los cuales se pueden acceder son los datos personales que podrían ser vulnerados por informaciones de carácter público, en virtud de que la protección de la persona contra el uso abusivo de los datos contenidos en los registros o bases de datos es uno de los fines fundamentales que tiene esta institución jurídica.

Desde un punto de vista teórico, se podría considerar que el hábeas data está diseñado para proteger uno o más derechos, sin que ello llegue a implicar que éstos sean de su exclusividad, ya que existen otras figuras aptas para proteger derechos ante diferentes supuestos. En este sentido, tenemos que el derecho a la reparación de los daños o el derecho al control de las actividades de los bancos de datos pueden ser protegidos, pero por medio de otros procedimientos judiciales diferentes al hábeas data.

En lo atinente a los derechos que se tutelan por medio de esta institución, la doctrina se encuentra dividida, ya que se ha sostenido que la tutela aludida se refiere, bien al derecho a la información, al derecho a la intimidad, al derecho a la identidad o al derecho a la autodeterminación informática.

En este sentido, parte de la doctrina sostiene que, debido al nacimiento de la informática y con ella el procesamiento de datos, existe la posibilidad de registrar una gran cantidad de datos sobre las personas que permiten reconstruir sus detalles íntimos y con ello afectar su vida privada o intimidad. Dentro de este contexto, se debe considerar al hábeas data como un mecanismo tendiente a proteger ese espacio íntimo de la persona, es decir, como una herramienta para defenderse de las intromisiones, tanto por parte del Estado como de los particulares.

Por ejemplo en Guatemala cuando un sujeto intenta corregir los datos falsos (ya sea en Infor.net, TransUnion, Crediref, Etc.) que se encuentran almacenados en los bancos de

datos o los registros, lo que se intenta realmente es tutelar la identidad del individuo frente a la sociedad. Esto es porque parte de la doctrina comparada estima que el hábeas data protege el derecho a la información.

El hábeas data para Guatemala debe representar una nueva garantía constitucional, puesto que tutela la libertad informática y con ella el derecho a la autodeterminación informativa, entendiendo a éste último como la facultad de la persona de decidir básicamente por sí misma cuando y dentro de qué límites procede revelar situaciones dentro de la propia vida. Es decir el hábeas data tutela y protege una serie de derechos personalísimos, por lo que todo dependerá de la situación en particular, así como de la concepción que se tenga dentro de cada ordenamiento jurídico.

Por lo anterior, todo guatemalteco y por lo establecido en el Artículo 31 de la Constitución Política de la República de Guatemala, debería tener:

1. El derecho de conocer sobre la existencia de registros sobre su persona.
2. El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas.
3. El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él.
4. El derecho de conocer el uso y finalidad que hace de la información quien la registra.
5. El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo.
6. El derecho a la rectificación del dato falso o incompleto.
7. El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas”.

Por lo anterior, se evidencia la necesidad de crear una norma que sancione quien no considere el hábeas data como un derecho como una acción. Si se parte de una concepción restringida, se podría concluir que será necesario que la Asamblea Nacional Constituyente legisle sobre la materia para poder determinar los efectos de

dicha acción, pero vía interpretación analógica, se puede concluir que se podría aplicar el procedimiento de amparo.

La Carta Magna otorga en sentido amplio el derecho a acceder a la información y al conocimiento del fin, pero se trata de derechos que han de ser ejercidos previamente (incluso extrajudicialmente y tal vez hasta por vía administrativa en algunos casos) ante el recopilador real o supuesto, naciendo la lesión al titular de los derechos de ese ejercicio extrajudicial fallido (ante el órgano administrativo que controla el dato personal). Ante tal situación, la víctima puede optar entre un juicio ordinario para hacer valer su derecho negado, acumulando pretensiones, o bien por medio de un amparo si se dan los supuestos para su procedencia.

En este orden de ideas, se concibe que, para intentar un amparo se debe fundar la demanda en la existencia cierta de un sistema de información que lleva una persona, dentro del cual existen datos e informaciones referentes al accionante (datos e informaciones en plural, es decir, varios que permiten delinear en alguna materia un perfil de la persona, o de sus bienes). Mediante el amparo se puede ejercer el derecho a acceder ante la petición de acceso extrajudicial negado ilegítimamente y que se concreta judicialmente mediante una exhibición, en caso de que una lesión de la situación jurídica del accionante se va a consolidar irremediabilmente por la negativa del acceso.

El problema no es tanto que la Constitución Política de la República de Guatemala faculte al individuo de conocer su información, porque en lo concerniente al derecho a conocer el uso y finalidad de la recopilación, no es en principio el amparo una acción que permite la satisfacción plena de este derecho, ya que quien tiene la información es realmente quien en su fuero interno conoce para qué la maneja y cómo la va a usar, e indagar tal propósito, no es materia de amparo. Por ello lo sancionatorio debe ser el uso y finalidad de los datos se pondera sólo en el sentido de declarar legal o ilegal lo que realiza el recopilador, no siendo tal declaratoria motivo de amparo, sino de una acción ordinaria o autónoma de hábeas data.

Cuando exista prueba fehaciente de la existencia del registro y de que en él se guardan informaciones y datos sobre el accionante, como parte de su contenido, así como del uso o fin ilegal que se hace de ellas en perjuicio del actor, si es que ello origina en su situación jurídica una lesión que de inmediato va a convertirse en irreparable o una amenaza inminente de lesión la cual también debe ser sancionada.

4.1. Definición

“Se conoce como hábeas data a la acción legal que tiene un sujeto para acceder a un registro o banco de datos que incluye información sobre su persona. El individuo tiene derecho a exigir la corrección de los datos en caso que estos le generen algún tipo de perjuicio o que sean erróneos. El Hábeas Data ha sido reglamentado por la legislación de numerosos países y también se encuentra contemplado en normativas de protección de los datos personales. Argentina y España, entre otras naciones, cuentan con organismos de control que supervisan el manejo de los datos personales que realizan las empresas privadas y las instituciones públicas”.⁴⁵

El hábeas data, por lo tanto, supone una garantía sobre el adecuado manejo de la información personal que se encuentra bajo poder de terceros. Esto permite evitar los abusos y subsanar los errores involuntarios en la administración y publicación de los datos.

Este recurso legal suele ser muy importante en lo referente a la información financiera. El hábeas data habilita a una persona a conocer su propia historia de crédito y a saber a quiénes se les ha suministrado dicha información. El sujeto también puede exigir que, una vez que se haya cumplido el periodo de caducidad de la información, se borre toda la información negativa sobre su historia crediticia, por ejemplo.

⁴⁵ <http://definicion.de/habeas-data/>

El recurso de hábeas data también ha sido utilizado por personalidades públicas como modelos y actrices que exigieron la eliminación de sus nombres en buscadores de Internet que vinculaban dicho dato a contenidos pornográficos entre otros.

El hábeas data es un derecho humano de naturaleza procesal que permite a cualquiera acceder a bancos o registros de datos, públicos o privados, computarizados o no, que contengan información sobre su persona, con la finalidad de tomar conocimiento, ya sea sobre su contenido, para identificar a la persona que proporcionó el dato, los motivos de su almacenamiento o el lugar donde se pueda ubicar; o bien para modificarla agregando información no contenida en procura de actualizar el registro o corregir la información equivocada o falsa; suprimir aquella que afecta la intimidad personal u otros derechos fundamentales. Asimismo, para impedir el acceso de terceros a información clasificada; denegar su uso en el marco de un proceso judicial o supervisar el soporte técnico en el almacenamiento de los datos garantiza su confidencialidad, o impugnar la interpretación, el análisis o la valoración equivocada de los datos. También sirve para permitir el acceso a la información que obra en las entidades de la administración pública y que le es negada al agraviado.

El hábeas data es una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

El hábeas data es un mecanismo e instrumento procesal de carácter constitucional que busca tutelar el acceso a la información pública y autodeterminación informativa como medio para acceder, modificar, actualizar y corregir toda información personal o de interés público contenida en registros de entidades públicas y privada.

En una primera aproximación, el hábeas data pueden ser clasificados paralelamente en:

- a) **“Propios:** Estos se consideran por estar ejercidos en estricta conexión con el tratamiento de datos de carácter personal e impropios utilizados para resolver

problemáticas conexas, pero bien diferenciables, como el acceso a la información pública o el ejercicio del derecho de réplica.

- b) **Individuales y Colectivos:** Según si es ejercido a título personal o en representación de un número determinado o indeterminado de personas.
- c) **Preventivos:** Estos persiguen evitar daños no consumados y reparadores, cuyo objetivo es el de subsanar daños ya proferidos o que se están ocasionando.
- d) **Ortodoxos:** Son los estrictamente relacionados con las facultades ordinariamente conferidas a los titulares de los de datos para operar sobre éstos y Heterodoxos los que exceden dicha tipología y que generalmente son inferidos de los principios básicos de la protección de datos, como aquellos que pudieran ser articulados por el defensor del pueblo, en tutela de derechos de incidencia colectiva, o por los responsables o usuarios de bancos de datos, articulados respecto de otros responsables o usuarios a quienes le cedieron la información y la están tratando ilegítimamente allí estarían tutelando derechos propios y de los registrados⁴⁶.

4.2. Datos personales

Los datos personales de los individuos han cobrado relevancia en el sistema financiero guatemalteco debido a los avances tecnológicos en la recopilación de información y por el surgimiento de bancos de datos relacionados con información crediticia.

En aras de proteger a la persona contra los abusos con relación a su esfera de intimidad surgió el hábeas data, como se ha hecho mención a lo largo de este trabajo, es una institución que proporciona el derecho a toda persona de conocer que datos propios constan en registros de bancos de datos, en registros privados, destinados a proveer informes, para pedir su supresión, rectificación, confidencialidad o actualización en caso de falsedad o discriminación.

⁴⁶ Ekmekdjian, Miguel Angel y Pizzolo, Calogero. **Habeas**, pág. 61.

Aplicaciones como buscadores, redes sociales, servicios de correo electrónico son poderosas y valiosas herramientas hoy en la sociedad de la información, pero no exentas de riesgos.

Ante el incremento de este tipo de servicios es necesario que los usuarios de la red, conozcan sus derechos y obligaciones, y los posibles peligros a los que se enfrentan, para que puedan hacer un uso seguro y responsable de las mismas.

Esta nueva ley de protección de datos personales que se ha venido proponiendo exige que todo aquel que efectúe operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relevamiento, evaluación, bloqueo, destrucción, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, interconexiones o transferencias, debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento de este tipo de información, pero sobre todo que la misma sea para beneficio y no para perjudicar a los propietarios de la misma.

La misma debe ofrecer las garantías necesarias para resguardar la seguridad y confidencialidad de los datos personales, a modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En la historia del derecho se encuentran diversos tipos de influencias que han marcado un cambio trascendental en el campo de aplicación y en el desarrollo de esta ciencia, pero han sido tres inventos que han marcado un cambio influyente, la escritura, la imprenta y la computadora. Esta idea es más amplia por lo indicado por Cáceres y Sánchez al citar a Lozano y señalar que la historia del derecho *“está condicionada por las tres revoluciones, de la escritura, de la imprenta y de la ordenación electrónica de datos.* Cada una de ellas en su momento marco un antes y un después en el Derecho, y cada uno de ellos al principio tuvo sus impulsores y sus detractores. Hoy en día

vemos a la escritura y la imprenta como algo común, pero es fácil imaginar los problemas que tuvo que solventar la imprenta de Johannes Gutenberg (S. XV) en su época, los cuales se quedan atrás con los que tiene que enfrentar la computadora”.⁴⁷

Con los actuales avances tecnológicos los problemas que la computadora está teniendo con la ciencia del derecho son innumerables pero tienen un origen común, desde el punto de vista, que no es la computadora el fin sino el medio, se le ha olvidado a algunos de los estudiosos del derecho porque del surgimiento de la computadora, como en su momento vieron los monjes escribanos a la imprenta.

La escritura en su momento permitió un desarrollo trascendental para el derecho, al poder dejar plasmado el conocimiento y estudiarlo en un futuro para mejorarlo; ya no tenía que transmitirse verbalmente de generación en generación, con la posible incorrecta interpretación del conocimiento, de la información.

La tecnología de la información puede ser definida como el conjunto de conocimientos en materia informática utilizados para el manejo de toda clase de información, auxiliándose de los medios y avances en materia de comunicación (televisión, radio, telecomunicaciones, Etc.) y el desarrollo de la computación en cuanto al procesamiento automático de la información.

Por supuesto que las tecnologías de la información y especialmente la internet están innovando en el conocimiento humano y en la sociedad en general, por ello el derecho tiene un nuevo reto, el cual se debe regular por el mal aprovechamiento o malversación con la tecnología.

⁴⁷ Sánchez Montenegro, Diego. **El Derecho de acceso a la información pública y su vinculación con las nuevas tecnologías de la información y la comunicación.** En: IV Congreso mundial de Derecho Informático. AEDIT, pág. 15.

4.3. Amenazas tecnológicas

En el Artículo 20 de la Declaración Universal de Bioética y Derechos Humanos en evaluación y gestión de riesgos, establece: “Se deberían promover una evaluación y una gestión apropiadas de los riesgos relacionados con la medicina, las ciencias de la vida y las tecnologías conexas”.

Es necesario tener una interpretación correcta de los riesgos y sobre todo de la amenaza de una posible extinción de la especie humana.

Con relación a este tema existen tres tipos de extinción humana y sus riesgos o amenazas:

1. **“Directa:** Dado el desarrollo actual de la tecnología podría suceder: una confrontación bélica, actos terroristas, tecnologías fuera de control, los cuales podrían llevar a la extinción de la especie humana (destrucción del planeta).
2. **Indirecta:** Producto de la dependencia de las tecnologías en un mundo ambicioso y egoísta basado en el poder hegemónico, la competencia y el súper consumismo, se hace inevitable el desarrollo incontrolable de la tecnología y su mal uso, trayendo como consecuencia el aumento de la contaminación del medio ambiental (degradación del planeta).
3. **Autoextinción:** Dado la filosofía del tener y el vacío espiritual, la tecnología comenzara a invadir cada vez más el contexto humano por medio de prótesis, implantes, sustitución de órganos con el fin de romper con los límites humanos, lo cual llevara al auto exterminio de la especie humana en aras de una nueva especie no humana (degradación de la naturaleza humana)”.

Estamos en la era de la tecnología y son muchos los que abrazan posiciones tecnofuturistas y creen que la solución a todos los problemas humanos están en la ciencia y la tecnología y afirman que la solución, esta exclusivamente, en el desarrollo acelerado de la tecnología. Lo que quiere decir que debemos concentrar todos nuestros esfuerzos en desarrollar instrumentos, aparatos y máquinas cada vez más

potente. La idea consiste en acelerar la tecnología para alcanzar una superinteligencia y luego fundirse con ella.

La ideología de los futuristas tecnológicos se fundamenta en tres premisas:

- “Se sustenta en una ideología que sustituye a la fe religiosa al prometer, curar a las enfermedades, eliminar la vejez, alcanzar la vida eterna... Alcanzar el paraíso en la tierra.
- Convencimiento de que el fin de la humanidad es inevitable y hay que intervenir y crear una nueva evolución artificial basada en la tecnológica.
- Convencimiento de que la tecnología por si sola es capaz de resolver todos los problemas actuales de contaminación, pobreza, desigualdades, guerras”.⁴⁸

“La singularidad plantea que el desarrollo de las maquinas es exponencial y su capacidad se duplica a una velocidad acelerada, lo cual conducirá a que las maquinas alcancen la capacidad del cerebro humano y luego la superen y afirman que esto debe acontecer a partir del 2025. Dado lo inevitable de este proceso, los futuristas tecnológicos afirman, que sólo nos queda una alternativa fundirnos con la máquina. Proceso que será de forma paulatina, por medio de prótesis, implantes de chip en el cerebro, copias de zonas del cerebro, Etc”.⁴⁹

“El transhumanismo es una ideología que trae nuevas esperanzas con matices religiosos de redimir al ser humano de su sufrimiento y promete alcanzar la gloria en la tierra. Lo preocupante es que hasta el momento no existe alguna alternativa sobre el futuro que tenga el encanto de la visión transhumanista.

Con respecto a la aceleración tecnológica, podemos no estar de acuerdo con el escenario de una singularidad que nos lleve a la fusión entre humanos y tecnología.

⁴⁸Bustamante, Javier, **Sociedad informatizada: ¿Sociedad deshumanizada?** 1994.
<https://sites.google.com/site/cibernetcamatematica/ensayos/los-desafios-del-siglo-xxi>

⁴⁹Ibid

Pero, dado el desarrollo actual es innegable que se están produciendo estos tres factores:

1. La aceleración tecnológica es una realidad. Antes llevar a la práctica una teoría llevaba años, hoy lleva meses, mañana llevara días u horas.
2. Integración (más bien invasión) de las tecnologías en la naturaleza, la sociedad y en nuestras vidas es cada vez mayor.
3. La convergencia de las tecnologías y la sinergia entre nano, bio, info y cogno (NBIC) Lo cual traerá un impacto de consecuencias impredecibles⁵⁰.

Tampoco se puede negar el hecho de que la tecnología es cada vez más autónoma e inteligente.

Subestimar el impacto de la tecnología. Concentrarse solamente en la degradación del planeta sin tener en cuenta la aceleración tecnológica. Subestimar el desarrollo tecnológico, seguir pensando que es sólo una herramienta y creer que la tecnología siempre estará bajo nuestro control, sin tener en cuenta los intereses mercantiles y hegemónicos que se mueven detrás de la tecnología así como ignorar la ideología transhumanista y su poderosa visión de futuro, el no tener en cuenta la campaña de promoción y posicionamiento en la mente humana, que se está llevando a cabo sobre la singularidad tecnológica y sobre todo ignorar el impacto social, económico, político y militar que tendrán las tecnologías convergentes (NBIC) sobre el futuro de la humanidad.

Tal negligencia y falta de visión de futuro, llevará a una degradación cada vez mayor del planeta y a la extinción indirecta de la humanidad.

Aceptar a la tecnología como la salvadora del planeta y apostar todo a la aceleración tecnológica (singularidad) Lo cual nos llevara al transhumanismo, Pero dentro del contexto actual de poder, lo único que hará es que unos sean más poderosos que

⁵⁰ <http://cibernetica.wordpress.com/page/2/>

otros, aumentando la desigualdad, ahora entre transhumanos y humanos. Dado su carácter ideológico los pobres también serán convertidos a obsoletas versiones de transhumanos. Priorizar la aceleración tecnológica por encima de la degradación del planeta lo cual conducirá a que la evolución natural sea sustituida por una evolución artificial que terminará en la autoextinción de la humanidad.

Buscar la integración armónica (no invasiva) de la tecnología en el contexto humano, basado en la cooperación (en lugar de la fusión) entre humanos y tecnologías. Se busca poner la aceleración tecnológica en función del desarrollo intelectual y espiritual de los humanos. Que vaya a las causas de la degradación y potencie la integración armónica de la tecnología a la naturaleza, la sociedad y el mejoramiento humano. Buscar alternativas que permitan lograr una sostenibilidad tecnológica (en lugar de una singularidad) basada en principios éticos universales que permitan formar generaciones cada vez mejores, basadas en la manifestación plena del ser.

Ahora bien, que tiene que ver todo lo anterior con el actual estudio, simple, comprender que la tecnología está inmersa en el que hacer de cada día, que ninguno de nosotros esta libre o aislado de la amenaza tecnológica, por eso es posible averiguar donde está ubicada una persona físicamente por medio del modem de su laptop. Con el avance de la tecnología, los usuarios pueden ser fácilmente vulnerados en su privacidad. El uso de herramientas como redes sociales se convierte en una carta abierta sobre la información de su dueño.

Según un estudio de la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Tecnologías de la Comunicación (Inteco) recogido por el sitio web sociedad de la información, el registro, el propio desarrollo de la actividad y el momento de darse de baja del servicio son los tres espacios en los cuales los datos personales del usuario están en mayor riesgo.

Eso no es todo. El teléfono móvil puede también ser una amenaza en contra de su propio dueño si no se toman las precauciones necesarias. El uso de los teléfonos inteligentes, hoy en día utilizados como un computador personal, aumenta la

exposición a riesgos de seguridad tales como el robo, el extravío o la invasión de la privacidad.

Es por ello que en la actualidad se recomienda activar el temporizador de bloqueo automático para evitar que un desconocido tenga acceso libre al dispositivo. Asimismo, se debe cambiar constantemente la clave de bloqueo para evitar intromisiones. Por otro lado, dejar activada la herramienta de bluetooth y con acceso libre para todos los dispositivos puede de igual manera representar un riesgo, por lo que se aconseja activarla sólo cuando el usuario lo requiera.

Encriptar los datos (protección de los mismos) en la memoria de teléfono o computadora es un mecanismo útil en caso de robo. Expertos en tecnología recomiendan, además, que al momento de descargar contenidos el usuario conozca el certificado de la aplicación, a fin de evitar la intromisión de piratas.

4.4. El derecho de las personas investigadas

A lo largo de este estudio se ha dicho del robo de identidades, de compra venta de datos de carácter personal, como puede defenderse las personas que están siendo objeto de estas acciones cuando desconocen sus derechos. Por parte del gobierno se debe de crear campañas de concientización en el uso de la tecnología en la protección de sus datos con recelo.

“En el año 2009 se presentaron muchas denuncias a la Procuraduría de los Derechos Humanos derivado que empresas privadas contrabandean información calificada de carácter personal, luego la comercializan. Estos actos se suman a que las entidades bancarias en varias ocasiones para presionar a los clientes con el pago los amenazan con colocar su imagen crediticia en Infor.net, TransUnion, Crediref, o cualquier otra con quien tengan contrato, es decir, que la banca guatemalteca forma parte de esta red de información que se mueve clandestinamente sin que los guatemaltecos se den cuenta que sus datos están siendo contrabandeados y comercializados, vedándoles, en la

mayoría de los casos, el derecho de rectificación como lo establece el Artículo 31 de la Constitución Política de la República de Guatemala, por ignorar en muchas ocasiones dichas transacciones de información”.⁵¹

El problema es que las personas no tienen el derecho de defensa, ya que no existe una norma que sancione este acto como delito y, al no estar tipificada esta figura no puede haber sanción para quien realice tales actos por parte de quien vende la información como quien la compra.

Desde el año 2003 se ha ventilado un caso en contra la empresa Infor.net la misma se inició a raíz de una denuncia interpuesta por un medio de comunicación. En esa ocasión el equipo de cómputo de la compañía quedó bajo custodia en su oportunidad se indicó que en 38 ocasiones se intentó efectuar un peritaje del contenido de esos archivos; pero por razones que nunca explicaron no lo habían logrado.

Con esa actuación se logró demostrar que esas bases de datos limitan el derecho de las personas, ya que estaban desactualizadas. Dicha desactualización conlleva consecuencias dramáticas, como no poder recibir un crédito u obtener un trabajo, porque cuando revisan las bases compradas, las personas están registradas con problemas que en muchos casos ya han solucionado.

No es secreto para nadie que existen instituciones y personas que venden información y que están conscientes de que es un acto ilegal. Dichos datos provienen de fuga de información en registros como el de la banca y comercio; juzgados, la policía y el Instituto Guatemalteco de Seguridad Social, bancos.

Una de las técnicas más conocidas es la que emplean los abogados, por medio de la Internet, para enterarse de las demandas que ingresan en el Organismo Judicial. Para esto deben estar suscritos a empresas que venden tal información privada, entre ellas, Infor.net, TransUnion, Crediref, Etc.

⁵¹ Informe anual. Procuraduría Derechos Humanos Guatemala, 2010

En dichas bases de datos se encuentra información de cuánto gana una persona, en qué trabaja, quiénes son los hijos, nombre de la esposa, número de cédula, si es propietario de casa o se ha cambiado de residencia. Hay abusos en la divulgación de los datos privados de los guatemaltecos, por lo que se debería combatir. Se atropella la privacidad y esto sólo se puede lograr creando una ley de protección de los datos personales.

La identificación de las personas se conoce en varias instituciones, entre ellas, bancos y entidades de crédito, donde saben todo acerca de uno, por ejemplo dónde trabaja, cuánto gana, dónde se tienen cuentas bancarias y cuántos hijos tiene.

En las instituciones públicas se tenía en reserva la información, pero, como los funcionarios manejan fondos del Estado, se necesita transparentar su uso. Hay que tener cuidado con el crimen organizado, porque ellos están muy bien informados y, en el caso de los funcionarios, esto los hace vulnerables a extorciones.

Ese historial, a veces, perjudica y desde hace una década muchos guatemaltecos han sufrido una serie de atropellos por este tipo de acciones que si se tipificaran en el Código Procesal Penal como una violación a la privacidad de las personas, y pueden ser causales y ser objetos de robos, extorciones y otra clase de delitos que se generan a través de la obtención de información.

4.5. Situación actual en la seguridad de información

En el mundo comercial, la información se ha constituido en un bien sumamente valioso y codiciado...hasta el punto de buscarlo y quererlo recoger por cualquier medio, por parte de compañías y empresas (por ejemplo: por encuestas fútiles, a través de constancias de asistencia, comprando bases de datos ajenas, Etc.). En ocasiones se busca la identificación, existencia y ubicación de las personas; otras veces, datos más difícilmente accesibles como ocupación, lugar de trabajo, zona de residencia...y hasta gustos (tal y como se puede encontrar uno a través de esos inocentes test de

Facebook). Uno de los principales elementos manejados en el área financiera de hecho, es la información, tanto de los usuarios como de valores, y, especialmente, de clientes titulares y potenciales.

La mala administración de éstos datos, el abuso con los mismos de diversas formas (como el retardo de la información, el manejo a espaldas de la información propia, la distribución abusiva de la misma y demás) y la ausencia de una base normativa sistemática en el país para proteger la información de cada uno de los guatemaltecos precipitó la expedición de una ley para el ejercicio del hábeas data proclamado en el Artículo 31 de la Constitución Política de la República de Guatemala: Esa ley fue la del Decreto 57-2008, Ley de Acceso a la Información Pública que, a pesar de todos los problemas y la existencia de lagunas, hoy se encuentra finalmente vigente.

En Guatemala existen aproximadamente ocho empresas que se dedican a la comercialización y contrabando de datos de carácter personal. Las mismas incumplen ciertos puntos que son importantes hacer mención:

La calidad o veracidad de los datos: La información contenida en los bancos de datos muchas veces no es veraz, está incompleta, no es exacta, no está actualizada, es improbable e incomprensible.

La finalidad informada: La administración de datos personales debe obedecer a una finalidad legítima y legalmente válida, la cual debe ser informada al titular de la información previa o concomitantemente con el otorgamiento de la autorización cuando ella sea necesaria, o siempre que el titular lo pida.

La circulación restringida: La circulación de la información del titular que no sea pública debe obedecer a la finalidad con la cual se recibió y no puede ser posteriormente replicada.

La temporalidad de la información: Si la información que se tiene del titular no es positiva, no puede permanecer por siempre.

La confidencialidad: Todos los que manejen datos deben garantizar la reserva de los mismos, incluso después de terminado el propósito de su uso.

La seguridad de los datos: No existen medios técnicos y protocolos necesarios para evitar el daño, adulteración, filtración y pérdida de la información del titular.

Y la interpretación integral de los derechos constitucionales son principios dirigidos a la protección de la reputación y buen nombre de los dueños de los datos o titulares (como los denomina el Hábeas Data). Frente a este principio quepa señalar que el derecho a la información no puede ser bandera de abuso para ir por encima de los derechos de la intimidad y buen nombre de los titulares de los datos.

El Gobierno debe legislar una norma donde se establezca la forma en la cual los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deban presentar la información de los titulares de la información.

En la actualidad el robo de datos personales se da por medio del phishing, el problema del uso de esta técnica es que los datos son enviados en servidores de diferentes partes del mundo y es allí, donde se encuentra el verdadero problema al querer proteger a los usuarios y su información.

Entrando más a detalle el phishing consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador o traficantes de información.

Existe un amplio abanico de software y aplicaciones de toda índole que quedan clasificados dentro de la categoría de robo de información personal o financiera,

algunas de ellas realmente complejas, como el uso de una ventana flotante sobre la barra de direcciones del navegador con el fin de confundir al usuario.

Algunas de las características más comunes que presentan este tipo de mensajes de correo electrónico son:

Uso de nombres de compañías ya existentes: En lugar de crear desde cero el sitio web de una compañía ficticia, los emisores de correos con intenciones fraudulentas adoptan la imagen corporativa y funcionalidad del sitio web de una empresa existente, con el fin de confundir aún más al receptor del mensaje.

Utilizar el nombre de un empleado real de una empresa como remitente del correo falso: De esta manera, si el receptor intenta confirmar la veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.

Direcciones web con la apariencia correcta: Como se hizo mención, el correo fraudulento suele conducir al lector hacia sitios web que replican el aspecto de la empresa que está siendo utilizada para robar la información. En realidad, tanto los contenidos como la dirección web (URL) son falsos y se limitan a imitar los contenidos reales. Incluso la información legal y otros enlaces no vitales pueden redirigir al confiado usuario a la página web real.

Debido al factor miedo: La ventana de oportunidad de los defraudadores o los piratas de la información es muy grave, ya que una vez se informa a la compañía de que sus clientes están siendo objeto de este tipo de prácticas, el servidor que aloja al sitio web fraudulento y sirve para recoger información se cierra en el intervalo de unos pocos días. Por lo tanto, es fundamental para el defraudador el conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.

Para lograr su objetivo, este tipo de malware, como se le conoce en el medio informático, además de la ocultación de la URL fraudulenta en un correo electrónico aparentemente real, también utiliza otras técnicas más sofisticadas:

“Man-in-the-middle (hombre en el medio). En esta técnica, el atacante se sitúa entre el usuario y el sitio web real, actuando a modo de proxy (referencia a un programa o dispositivo que realiza una acción en representación de otro). De esta manera, es capaz de escuchar toda la comunicación entre ambos. Para que tenga éxito, debe ser capaz de redirigir al cliente hacia su proxy en vez de hacia el servidor real. Existen diversas técnicas para conseguirlo, a modo de ejemplo por no ser el fin de esta investigación todo se hará grosso modo, los proxies transparentes, el DNS Cache Poisoning (Envenenamiento de Caché DNS) y la ofuscación del URLs.”⁵²

Aprovechamiento de vulnerabilidades de tipo Cross-Site Scripting en un sitio web, que permiten simular una página web segura de una entidad bancaria, sin que el usuario pueda detectar anomalías en la dirección ni en el certificado de seguridad que aparece en el navegador.

Aprovechamiento de vulnerabilidades de Internet en el cliente, que permiten mediante el uso de exploits falsear la dirección que aparece en el navegador. De esta manera, se podría redirigir el navegador a un sitio fraudulento o pirata, mientras que en la barra de direcciones del navegador se mostraría la URL del sitio de confianza. Mediante esta técnica, también es posible falsear las ventanas pop-up abiertas desde una página web auténtica.

Algunos ataques de este tipo también hacen uso de exploits en sitios web fraudulentos que, aprovechando alguna vulnerabilidad de Internet o del sistema operativo del cliente, permiten descargar troyanos de tipo keylogger que robarán información confidencial del usuario.

⁵² <http://www.virus-seguridad/virus-seguridad2.shtml>

Otra técnica más sofisticada es la denominada Pharming. Se trata de una táctica fraudulenta que consiste en cambiar los contenidos del DNS (Domain Name Server, Servidor de Nombres de Dominio) ya sea a través de la configuración del protocolo TCP/IP o del archivo lmhost (que actúa como una caché local de nombres de servidores), para redirigir los navegadores a páginas falsas en lugar de las auténticas cuando el usuario accede a las mismas a través de su navegador. Además, en caso de que el usuario afectado por el pharming navegue a través de un proxy para garantizar su anonimato, la resolución de nombres del DNS del proxy puede verse afectada de forma que todos los usuarios que lo utilicen sean conducidos al servidor falso en lugar del legítimo.

El mecanismo más habitualmente empleado es la generación de un correo electrónico falso que simule proceder de una determinada compañía, a cuyos clientes se pretende engañar. Dicho mensaje contendrá enlaces que apuntan a una o varias páginas web que replican en todo o en parte el aspecto y la funcionalidad de la empresa, de la que se espera que el receptor mantenga una relación comercial. Si el receptor del mensaje de correo efectivamente tiene esa relación con la empresa y confía en que el mensaje procede realmente de esta fuente, puede acabar introduciendo información sensible en un formulario falso ubicado en uno de esos sitios web.

En cuanto a su distribución, también presentan características comunes:

De la misma manera que el spam, es enviado masiva e indiscriminadamente por correo electrónico o sistemas de mensajería instantánea:

El mensaje insta al usuario a pulsar sobre un enlace, que le llevará a una página en la que deberá introducir sus datos confidenciales, con la excusa de confirmarlos, reactivar su cuenta, Etc. Se envía como una alerta de una entidad financiera advirtiéndole de un ataque. Incluye un enlace que se insta a pulsar y en el que se solicitan datos personales.

Dado que el mensaje se distribuye masivamente, alguno de los receptores será efectivamente cliente de la entidad. En el mensaje se indica que, debido a algún problema de seguridad es necesario acceder a una dirección web donde debe reconfirmar sus datos: nombre de usuario, contraseña, número de tarjeta de crédito, PIN, número de seguridad social, Etc.

Por supuesto, el enlace no dirige a ninguna página de la compañía, sino más bien a un sitio web desarrollado a propósito por los estafadores o piratas y que reproduce la imagen corporativa de la entidad financiera en cuestión. Normalmente la dirección web contiene el nombre de la institución legítima por lo que el cliente no sospecha de la falsedad de la misma.

Cuando el usuario introduce sus datos confidenciales, éstos se almacenan en una base de datos y lo que ocurre a continuación no necesita de un gran esfuerzo de imaginación: los estafadores utilizan esta información para conectarse a su cuenta y disponer libremente de los fondos.

Los principales daños provocados por el phishing son:

- Robo de identidad y datos confidenciales de los usuarios.
- Pérdida de productividad.
- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, Etc.).

Para poder distinguir un mensaje de phishing de otro legítimo no resulta fácil para un usuario que haya recibido un correo de tales características, especialmente cuando es efectivamente cliente de la entidad financiera de la que supuestamente proviene el mensaje.

El campo De: del mensaje muestra una dirección de la compañía en cuestión. No obstante, es sencillo para el estafador o pirata modificar la dirección de origen que se muestra en cualquier cliente de correo.

El mensaje de correo electrónico presenta logotipos o imágenes que han sido recogidas del sitio web real al que el mensaje fraudulento hace referencia.

El enlace que se muestra parece apuntar al sitio web original de la compañía, pero en realidad lleva a una página web fraudulenta, en la que se solicitarán datos de usuarios, contraseñas, Etc.

Normalmente estos mensajes de correo electrónico presentan errores gramaticales o palabras cambiadas, que no son usuales en las comunicaciones de la entidad por la que se están intentando hacer pasar.

Todos los usuarios del correo electrónico corren el riesgo de ser víctimas de estos intentos de ataques. Cualquier dirección publicada en Internet (que haya sido utilizada en foros, grupos de noticias o en algún sitio web) será más susceptible de ser víctima de un ataque debido a los spiders que rastrean la red en busca de direcciones válidas de correo electrónico.

Éste es el motivo de que exista este tipo de malware. Es realmente barato el realizar un ataque de este tipo y los beneficios obtenidos son cuantiosos con tan sólo un pequeñísimo porcentaje de éxito.

El robo de identidad, de datos personales, de cualquier tipo de información está a la orden del día, cabe aclarar que con la creación de una simple norma no se evitará el contrabando, robo y comercialización de información. También se debe de crear un departamento especializado en informática para que esté monitoreando cadenas de información, su proveniencia, su asunto, tratando de intuir sus intenciones.

CONCLUSIONES

1. Según establece la Ley de Acceso a la Información Pública cualquier persona tiene acceso a la información que no sea confidencial ni reservada, sin importar su posición social o profesión. Pues la Ley no lo contempla, como tampoco la necesidad de justificar las razones por las que se está buscando la información.
2. El derecho a la información pública en La República de Guatemala está actualmente relacionado con la transparencia, pero el imparable avance tecnológico ha generado un nuevo problema ante el uso inadecuado que se haga de los datos de los ciudadanos, no existen garantías suficientes para ejercer sus derechos y sobre todo la protección de sus datos privados. Dado que de lo que se trata es que se haga un democrático uso de la tecnología de la información, más no la prohibición de la misma, porque sería prohibir el progreso.
3. Al no existir normativa respecto a la protección de los datos que se almacenan, investigan, recogen o transmiten por medios electrónicos. El cual es un derecho autónomo derivado del derecho a la vida privada, por consiguiente, es preciso indicar que no se garantiza una tutela específica frente a la creciente recopilación y almacenamiento de información puesto que se trata de una práctica potencialmente peligrosa para algunas personas con respecto al tratamiento de sus datos de carácter personal.
4. En los últimos años el debate en torno al tema de la protección de los datos de carácter personal ha adquirido una inusitada relevancia derivado de los problemas que se han desatado por empresas privadas que comercializan con información de la ciudadanía en general, en Guatemala no ha desarrollado aún una institución jurídica de índole constitucional como la acción de hábeas data, que garantice la pronta protección de la veracidad, la certeza jurídica y la confidencialidad de la información concerniente a las personas contenida en las bases y archivos de datos tanto de carácter público como privado.

5. Se considera una amenaza el avance tecnológico, al invadir gravemente la vida privada de las personas y de sus datos personales, al publicar en un registro privado con fines de lucro, información crediticia, bancaria, mobiliaria e inmobiliaria, etc. sin el previo consentimiento de la ciudadanía guatemalteca.

RECOMENDACIONES

1. Así como es de fácil solicitar información pública debiera ser fácil la protección de los datos de carácter personal, para ello el Congreso de la República de Guatemala, es indispensable aprobar en definitiva la iniciativa de ley, bajo el registro número 4090 Ley de Protección de Datos Personales y/o hacer una reforma a la actual Ley de Acceso a la Información Pública donde se tipifique específicamente la protección de los datos que sean considerados privados o reservados.
2. El Congreso de la República de Guatemala, debe de crear y aprobar una ley sobre protección de datos personales, por la razón de que otros países ya cuentan con éste ordenamiento jurídico, y por los diversos convenios internacionales como un derecho fundamental, que radica en la libertad del hombre, que se vería seriamente afectada por la invasión de su privacidad, violentando su propia conducta.
3. El Gobierno de Guatemala, debe asegurar y vigilar el cumplimiento, por parte de instituciones y organismos especializados en tecnología de protección de datos, el respeto de las disposiciones establecidas así como de cualquier otro acto que viole las libertades fundamentales, cuando las instituciones u organismos públicos y privados tratan los datos personales de los ciudadanos guatemaltecos.
4. Crear una Unidad Técnica adscrita a la Procuraduría de los Derechos Humanos que proporcione asesoría con la ayuda de los medios de comunicación a la ciudadanía, a las instituciones y a los organismos en relación a cualquier argumento relativo al tratamiento de datos personales, la vigilancia de los nuevos desarrollos que tienen una incidencia sobre la protección de los datos personales es de vital importancia, debido al acelerado cambio tecnológico que existe y las nuevas tendencias informáticas que ello implica.

5. El Congreso de la República de Guatemala, debe revisar otras leyes de carácter constitucional, para evitar que en el uso de este otro derecho constitucionalmente reconocido, se viole el derecho a la privacidad reconocido implícitamente en el Artículo 44 de la Constitución Política de la República de Guatemala y en otros artículos de La Carta Magna así como en convenios y tratados internacionales ratificados por Guatemala, con las excepciones de ley, tal es el caso de los actos realizados por funcionarios y empleados públicos en el ejercicio de sus cargos o en aquellos otros en donde las personas, en forma voluntaria, permitan injerencias en su vida privada.

BIBLIOGRAFÍA

AA.VV. **Ley sobre protección a la vida privada o protección de datos de carácter personal.** En: <http://www.sernac.cl/leyes/>

BARDELLI LARTIRIGOYEN, Juan B. **El derecho de Hábeas Data en el Código Procesal constitucional y en la jurisprudencia del tribunal Constitucional.** En: <http://www.riaj.org/>

BARZALLO, José Luís. Presidente AEDIT. Blog del Foro de Hábeas Data. En: **Ecuador: Ley de Protección de Datos.** Revista Jurídica Informática Mayo 30 de 2006.

BASTIAT, Frédéric. **La Ley.** Centro de Estudios Económico-Sociales. Guatemala. Universidad Francisco Marroquín 1995.

BELTRAMONE, Guillermo / ZABALE, Ezequiel. **El derecho en la era digital.** Editorial Juris. Santa fe. Argentina, 1997.

CARRASCOSA, Valentín. **Derecho a la Intimidad e Informática.** En Revista Informática y Derecho. UNED, Mérida, España, 1992.

CASTELLS, Manuel. **La ciudad informacional. Tecnología de la información, estructuración económica y el proceso urbano-regional,** Madrid Alianza Editorial, 1995.

Consejo de Europa, Asamblea Consultiva. Resolución N° 428. 23 de enero de 1970.

DAVARA RODRIGUEZ, Miguel Ángel. **Manual de Derecho Informático.** Editorial Aranzandi. Pamplona, España. 1997.

DE MORAGAS SPA, Miguel. **Semiótica y Comunicación de Masas,** Editorial Península, Primera Edición, Barcelona, España. 1976.

DE PINA VARA, Rafael. **Diccionario De Derecho.** Editorial Porrúa. México 1998.

EKMEKDJIAN, Miguel A./ PIZZOLO, Calogero. **Hábeas Data: Derecho a la Intimidad Frente a la Revolución Informática.** Editorial Lexis Nexis; Argentina; 2008

En Internet todo queda registrado, pág. 10, Prensa Libre (Guatemala), Año LIX, No. 19,473, lunes 1 de febrero de 2010, Guatemala.

GARCÍA HOZ, Víctor. **El nacimiento de la intimidad**. Editorial Rialp, Madrid 1950.

<http://buscon.rae.es/drael/>

GETTELL, R., **El pensamiento político en Grecia. Historia de las ideas políticas**, Editorial Labor Barcelona, 1930.

<http://informatica-derecho-juridico/informatica-derecho-juridico.shtml#constituy>, (10-01-2011).

<http://www.delitosinformaticos.com/propiedadindustrial/auditoria.shtml>, (10-01-2011).

<http://definicion.de/modelo-de-datos/>, (10-01-2011).

<http://delitosinformaticos.com/trabajos/hacking.pdf>, (10-01-2011).

http://www.darfruto.com/6_intimidad_privacidad.htm, (10-01-2011).

Informe anual. Procuraduría Derechos Humanos Guatemala, 2010

KORTH, Henry F. / SILBERSCHATZ, Abraham. **Fundamentos de bases de datos**. Mc Graw Hill; Mexico; 1993.

La Real Academia Española, www.rae.es/rae.html, (10-01-2011).

MARTI GARCÍA, Miguel-Ángel. **La intimidad**. EIUNSA, 1992.

PALAZZI, Pablo Andrés. **El Hábeas Data en el Derecho Argentino**. Lexis Nexis; Argentina; 2004.

PADILLA, Miguel M. **Banco de Datos y Acción de Hábeas Data**. Lexis Nexis; Argentina; 2008.

PÉREZ, Luís Aguirre. **Ponencia, el Uruguay impune y la memoria social en el Tribunal permanente de los pueblos, 1990, La impunidad en América Latina**, Sesión Uruguay, 20 al 22 de abril de 1990, Montevideo.

PÉREZ ROYO, Javier. **Curso de Derecho Constitucional**. Marcial Pons; Madrid, 2002.

Prensa Libre. **CC ordena destitución, Cesado Argueta, por rebeldía en cédulas**, pág. 2, (viernes 26 de febrero de 2010).
http://www.prensalibre.com.gt/edicion_empresa/pdf/

ROMERO SILVERA, Graciela. **Implicaciones jurídicas del desarrollo del derecho de acceso a la información pública, en el marco del derecho a la libertad de expresión y los derechos humanos**, International Law Review, 2011. Traducción libre.

SÁNCHEZ MONTENEGRO, Diego. **El Derecho de acceso a la información pública y su vinculación con las nuevas tecnologías de la información y la comunicación**. En: IV Congreso mundial de Derecho Informático. AEDIT, Junio, 2004.

SARTORI, Giovanni. **Homo videns: La sociedad teledirigida**, editorial Santillana-Tauros, Madrid, 1998, 160 páginas.

SENN, James A. **Análisis y Diseño de Sistemas de Información**. Mc Graw Hill; Mexico; 1992.

WARREN, Samuel D. y BRANDEIS, Louis. **The Right to Privacy**. Harvard Law Review, No. 5. Vol. IV. 15 de diciembre de 1890. Traducción libre.

YEPES STORK, Ricardo. **La persona y su intimidad**. Cuadernos de Anuario Filosófico, Servicio de Publicaciones de la Universidad de Navarra S.A., Pamplona, 1998 (2ª)

Legislación:

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

Declaración Universal De Derechos Humanos. Asamblea General de las Naciones Unidas, EEUU, 1948.

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

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

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

Constitución Política de los Estados Unidos de Norte América. Estados Unidos, 1986.

Constitución Portuguesa, 1976

Constitución Española, 1978

Constitución Política República Federativa de Brasil, 1988

Constitución Política de Colombia, 1991

Constitución Política del Perú, 1993

Constitución de la Ciudad de Buenos Aires, 1996