REPUBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

FACULTAD DE SEGURIDAD Y DESARROLLO

TRABAJO DE INVESTIGACION INDIVIDUAL

MAESTRIA SEGURIDAD Y DESARROLLO

"LA PROTECCION DE DATOS PERSONALES EN LA LEGISLACION ECUATORIANA"

DR. CARLOS ESPINOSA SEGOVIA

XII CSSD

2004 - 2005

REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

LA PROTECCION DE DATOS PERSONALES
EN LA LEGISLACION ECUATORIANA.

Autor: Doctor. Carlos Espinosa Segovia.
Asesor: Doctor. Enrique Gómez

Quito, 25 de Marzo del 2005.

AGRADECIMIENTO:

Al Instituto de Altos Estudios Nacionales, asesores, y en particular al Dr. ENRIQUE GÓMEZ, director del presente trabajo de investigación, por brindarme la oportunidad de culminar los estudios de Cuarto Nivel Académico y por la fructífera labor desplegada a favor de los profesionales del país.

DEDICATORIA:

A quienes más amo: mi cónyuge SANTA COLOMA-ROMERO y mis hijas: SOPHIA FERNANDA, joven profesional del Derecho, quien motivó el desarrollo de la presente temática, acorde a la modernidad, Y, a FRANCINITA, cuyos recuerdos se tornan cada vez más inolvidables, a pesar de su prematura partida.

LA PROTECCION DE DATOS PERSONALES EN LA LEGISLACION ECUATORIANA.

INTRODUCCION

La presente temática de investigación, ha despertado en mi el interés propio de llegar a puntualizar ciertas situaciones, que amparadas en el avance científico tecnológico, pueden ocasionar un verdadero caos en lo que respecta a la privacidad de la información de las personas en nuestra sociedad y determinar ciertos correctivos en base a reformas de orden legal a fin de coadyuvar a una correcta aplicación tecnológica preservando lo atinente a información reservada particular.

Hoy en día, los nuevos descubrimientos tecnológicos, particularmente en lo atinente al desarrollo a través de medios tecnológicos e informáticos, han logrado adentrarse en todos los campos del saber humano, constituyéndose inclusive en una herramienta diaria de trabajo dada su efectividad, alcance, operatividad y eficiencia en lograr sus fines.

Uno de los avances de mayor significación en el campo de la tecnología es la informática, que hace relación al manejo de la información, que en relación directa al desarrollo de la comunicación ha originado cierta interconexión entre las variadas latitudes del planeta, eliminando en si las fronteras de cada uno de los países, logros en base al internet, herramienta que permite a los usuarios comunicarse con los países del mundo alcanzando información de primera mano, lo que

facilita la realización de intercambio cultural, comercial, técnico, social, científico, artístico y de toda índole a nivel mundial.

Este desarrollo tecnológico, ha permitido el avance social y dentro de este campo, nuestra inquietud, el de tratar de mantener la privacidad de información para no atentar contra los Derechos Humanos, ni violar los derechos propios del hombre cual es la privacidad del ser, en base a la protección de datos personales.

No puede darse el caso, que personas inescrupulosas logren cierta información y que luego la reviertan en aplicaciones ilícitas perjudicando a terceros. Los datos personales son propios del ser y como tales merecen nuestro respeto, de allí, la necesidad de una legislación actualizada que garantice la seguridad de la información sobre la base de la confidencialidad de datos personales o situaciones de interés personalísimo del ser.

La presente tesis de investigación la desarrollaré en siete capítulos debidamente estructurados, así:
En su capítulo I bajo la denominación de **"El Derecho a la Información y el Derecho a la Intimidad"**, analizaré la trascendencia de la temática con relación a la protección de datos personales, partiendo de la concepción clara de su significado y señalando las características fundamentales de cada uno de estos derechos e identificar los parámetros en los que se desenvuelven, los cuales han ido adaptándose a los cambios sociales, partiendo de un derecho elemental a

la información conforme a la realidad de ese entonces y con un profundo respeto por parte de la sociedad a lo que se conceptualizaba como actos íntimos del ser.

En su capítulo II, bajo la denominación de **"la Informática y la Protección de Datos"**, me permitiré hacer un análisis conceptual de lo que implica la informática desde el punto de vista de avance tecnológico en nuestra era, destacando la importancia y el desarrollo de los distintos sistemas de información, estableciendo de esta manera, la forma en que la información va a ser generada, compilada y comunicada en la sociedad, de allí que en este capítulo se aborde el tema de las bases de datos, el almacenamiento de información y su utilización.

Además, el desarrollo del presente capítulo nos permitirá llegar a una clasificación de orden técnico de lo que implica datos y tipos de datos destacando su importancia y la necesidad de proporcionar garantías de orden jurídico sobre el manejo de la información en sociedad.

En el capítulo III, bajo el título **"Tratamiento de Datos Personales Procesados en Medios Electrónicos"**, se destaca las etapas que intervienen en el procesamiento de datos, muestra además los diferentes tipos de tratamiento de datos personales cuya determinación es indispensable para brindar una adecuada protección a esta información, así también, se expondrá las maneras de aplicación del procesamiento de datos en áreas específicas como son el internet, el comercio electrónico y las telecomunicaciones, definiendo los

stándares mínimos de protección de datos personales que se deberían considerar en el desarrollo y funcionamiento en cada uno de estos campos.

Bajo la temática **" El Hábeas Data, un instrumento insuficiente para la Protección de Datos Personales",** en el capítulo IV, definiré en qué consiste el Hábeas Data como institución Jurídica contemplada dentro de nuestra legislación, sus antecedentes de creación, para luego analizar su ámbito de aplicación y protección de derechos de las personas, y finalmente concluir, a título personal sobre la insuficiencia del Hábeas Data para lograr una protección efectiva de los datos personales y determinar la necesidad de crear una normativa específica en el contexto jurídico social, que permita adentrarnos a la información general del estado, sin atentar contra lo que constituye datos personales o mejor dicho personalísimos de la persona en sociedad.

Debo señalar además, que esta inquietud la manifesté al presentar el proyecto de Plan de Investigación de la presente tesis, y que de manera coincidente, a la fecha, el Estado Ecuatoriano, y en particular el Congreso Nacional aprueba la Ley de Transparencia y Acceso a la Información Pública, que si bien es cierto, hace relación a otro campo de la información como es el sector público, no es menos cierto que se halla ligado a situaciones de orden particular al referirse a personas inmersas en dicho sector del estado, tal es así, que en su artículo 6 hace relación a la información confidencial, definiéndola a la misma como aquella información

pública de carácter personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

Insisto en la necesidad de crear una normativa específica, que dentro de los parámetros del Hábeas Data, procure desarrollar este tema. Lo cual es posible, a través de la generación de definiciones que delimiten el alcance y sentido de la protección, así como el establecimiento de principios jurídicos que se constituyan en el referente de esta normatividad, con el único propósito de instaurar mecanismos prácticos, que garanticen una protección de datos personales eficaz y eficiente a favor de las personas y que a la par constituyan garantía plena para el libre desenvolvimiento y desarrollo de sus actividades en sociedad.

El Capítulo V, bajo la denominación de **"Principios Jurídicos aplicables a la Protección de Datos Personales"**, hace relación a los principios jurídicos fundamentales que se deben considerar para la realización de una norma jurídica, que proteja efectivamente los datos personales. De esta manera, estos principios constituyen referentes esenciales para alcanzar un procesamiento adecuado de esta información, a la vez que contemplan derechos y garantías de los titulares de datos personales.

El Capítulo VI. Que se refiere al **"Normativa Existente sobre Protección de Datos Personales"**, pone

de manifiesto el interés de los países del mundo, que atentos a la nueva era tecnológica, ha originado la creación de cuerpos normativos o legales tendientes a proteger los datos personales. No obstante, este capítulo se dedica exclusivamente, a destacar las mejores prácticas de legislación, que ya se encuentran vigentes, señalando además, que la protección de datos personales se origina desde 1919 con la constitución de Weimar. Por otro lado, además de enfocar las legislaciones nacionales existentes, se citan Convenios Internacionales, cuyo aporte ha sido relevante dentro del desarrollo normativo de este tema. Finalmente, se realiza una breve exposición de jurisprudencia, en la que se verifica el criterio de los Tribunales, el cual está orientado a salvaguardar y garantizar el derecho de los titulares de los datos personales.

Para concluir el presente Trabajo de Investigación, en sus capitulo VII, puntualizo las **"Conclusiones y Recomendaciones"** sobre la presente temática, señalando pautas, que me parecen razonables con el único objetivo de llegar a determinar ciertos correctivos para mantener la reserva de datos personales en sociedad.

CAPÍTULO

I

EL DERECHO A LA

INFORMACIÓN Y EL

DERECHO

A LA INTIMIDAD.

EL DERECHO A LA INFORMACIÓN Y EL DERECHO A LA INTIMIDAD.

Al abordar el tema de protección de datos personales es trascendental realizar un análisis previo sobre dos derechos que se relacionan con el tema, es el caso del derecho a la información y el derecho a la intimidad. El tratamiento legislativo que se dé a estos derechos es fundamental, ya que ambos deben complementarse y cubrir las áreas de protección más relevantes de cada uno, de tal manera que se dé una protección equilibrada a ambos.

I.1.a) DERECHO A LA INFORMACIÓN:

El Derecho a la Información es aquel que abarca los derechos y libertades referentes a la expresión y comunicación pública de datos. Así, lo estipula el artículo 19 de la Declaración Universal de los Derechos Humanos: "Todo individuo tiene derecho a la libertad de opinión y de expresión, este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

El Tribunal Constitucional español sostiene que. "la libertad de información juega un papel esencial como garantía institucional del papel democrático que inspira nuestra Constitución, el cual presupone el derecho de los ciudadanos a contar con una amplia y

adecuada información respecto a los hechos que les permita formar sus convicciones y a participar en la discusión relativa a los asuntos públicos. Es este aspecto el que puede explicar que este tipo de comunicados hayan aparecido en otros periódicos sin que ello haya motivado la intervención de la justicia penal, como se desprende de la documentación acompañada en autos." (Gozaíni, p. 49)

La Constitución Política del Ecuador en su Capítulo IV que habla de los derechos económicos, sociales y culturales, sección décima de la Comunicación, "Art. 81, determina que el Estado garantizará el derecho a acceder a fuentes de información; a buscar, recibir, conocer y difundir información objetiva, veraz, plural, oportuna y sin censura previa, de los acontecimientos de interés general, que preserve los valores de la comunidad, especialmente por parte de periodistas y comunicadores sociales", lo que implica que los individuos pueden gozar y ejercer este derecho en virtud del hecho de pertenecer a una sociedad organizada. De esta manera, presenta dos caras, una que se refiere al derecho que poseen los medios de comunicación para publicar y difundir sin restricciones la libertad de prensa; y la segunda es la que se enfoca al derecho individual de los seres humanos a estar informados sobre los datos que les concierne, que se encuentran archivados en una base de datos determinada.

El derecho a la información se encuentra constituido por tres libertades como son: la libertad

de investigar, la libertad de difundir y la libertad de recibir informaciones y opiniones.

Uicich establece que: Por libertad de investigar se entiende la posibilidad irrestricta de utilizar toda información obtenida legalmente y todos los medios existentes en procura de la información. La libertad de difundir es la consecuencia de la facultad de investigar. Toda esa información obtenida, en la medida que no perjudique el legítimo interés de terceros, goza de la facultad de ser difundida por cualquier medio de comunicación. La facultad de recibir información es la faceta pasiva de la ecuación.

Así como el ser humano, por ser tal, goza de la libertad de investigar y de difundir, él mismo es titular del derecho a ser informado, a exigir que la información le sea brindada (p.24). Pero, ¿Cuáles son los límites de este derecho a la información? ¿Qué prima, el derecho a la intimidad de las personas o la libertad de difundir, ideas, opiniones e información? Pierini al respecto señala que: "El derecho a informar, como todo otro derecho constitucional no es absoluto, sino que convive con otros derechos de idéntico rango a los cuales debe respeto." (p.172) De ahí, que se debe someter a valoración los datos, objetos de la información, con el fin de establecer si su difusión afecta los intereses legítimos de sus titulares, colocando a éstos en una situación de desventaja y vulnerando sus derechos.

Es así como, el art. 14.1 de la Convención Americana sobre Derechos Humanos establece que: "Toda

persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley." (Gozaíni, p. 51)

I.1.b) NUEVAS TECNOLOGIAS.

Las tecnologías originadas antes de la Segunda Guerra Mundial se relacionan con la automatización mecánica y se las identifican como tecnologías tradicionales.

Las nuevas tecnologías son las que surgieron con posterioridad, cuya evolución y desarrollo han sido de trascendencia fundamental para la sociedad, encontrando entre estas: -Biotecnologías, Nuevos Materiales y Tecnología de la Información.

BIOTECNOLOGIAS.- Significa la utilización integrada de principios científicos y tecnológicos para la obtención de bienes y servicios.

NUEVOS MATERIALES.- Constituyen la aplicación de nuevos procesos para el mejoramiento de materiales tradicionales y desarrollo de nuevos materiales o como también nuevos procesos o nuevos productos.

TECNOLOGIA DE LA INFORMACION.- La presente denominación agrupa todo lo relativo a creación, procesamiento y transmisión de señales digitales y la componen: harware, software, cibernética, sistemas de

información, redes, chips inteligentes, criptografía, robótica, inteligencia artificial y realidad virtual. Scott Morton, "The corporatións of the 1990´s,p.4 a 122. A la presente factorización que ha realizado el autor, se la agregado la criptografía y la realidad virtual, por considerarlas desarrollos salientes de la tecnología de la información.

Por considerarlo pertinente, me permito analizar varios temas de interés que hacen relación a las Tecnologías de la Información desde el punto de vista conceptual técnico.

a).- TEORIA GENERAL DE LOS SISTEMAS. (TGS).

Su creador fue el biólogo Von Bertalanffy, se basa en la función lingüística como una característica humana primaria y utiliza a los seres vivos como modelo primario de sistemas.

El enfoque inicial de su teoría, le permite partir de la concepción de un sistema abierto cognositivo de la realidad, que permite modificación del comportamiento del sistema, facilitando además el ordenamiento de las situaciones existentes desde el punto de vista global y más no particularizado de la realidad encaminándose a la existencia de una interrelación de sus componentes.

LA TGS, constituye una metodología para imaginar modelos integrales de los seres vivientes y, en particular , del hombre en sí mismo y en sociedad.

b).- LA CIBERNÉTICA.

El término cibernética la utilizó PLATON hace muchos años, para describir la ciencia que se ocupaba del control de la navegación de los barcos y, más tarde, para describir la ciencia o arte de que las personas podían valerse para preservar sus cuerpos y riquezas de los peligros que les acechaban.

AMPERE, la definía como la ciencia dedicada al control de la sociedad.

HEIDEGGER, habla de la Cibernética como una especie de culminación de la Filosofía.

A título ilustrativo, me permito señalar otras definiciones de Cibernética:

Disciplina científica que estudia los sistemas y procesos de comunicación y autorregulación, tanto en los seres vivos cuanto de los sistemas electrónicos y electromecánicos. (Océano Uno Diccionario Enciclopédico Ilustrado).

Estudio de las Analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas, y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la Tecnología. (Diccionario de la Lengua Española, Real Academia de la Lengua).

Ciencia encargada del control de las máquinas, organismos vivos y sociedades, así como de las señales de transmisión entre ellos. (Lorenzetti, Ricardo,

Comercio Electrónico, Editorial Abeledo - Perrot, Buenos Aires, 2001.

c).- PARADIGMA DE LOS SISTEMAS DE PROCESAMIENTO DE INFORMACION (SPI).(Información Process Systems).

Significa como un determinado procesador relaciona la información de entrada con la información de salida, en un ciclo de recursividad.

Vale decir, las instituciones sociales vistas como SPI proveen una relación estructurada de la manera en que las ideas pasadas reglan las acciones presentes y, también cómo las acciones presentes generan ideas futuras en un ciclo de recursividad contínuo de realimentación.

En sociedad, las acciones pasadas generan nuevas acciones para el presente y futuro.

Un SPI traduce las prácticas a teorías , mediante el proceso de codificación; las teorías a teorías , por medio del proceso de computación, y las teorías a prácticas , por el proceso de decodificación.

d).-COMPUTACION.

PENROSE" Shadows of the mind".- define como la actividad de un ordenador, pero en términos más precisos debe entenderse por tal, en un sentido convenientemente idealizado, la acción de una máquina de turing. de tal manera que nunca comete errores y puede funcionar tanto tiempo como sea necesario, con un espacio de almacenamiento ilimitado.

e).-INFORMATICA.

Constituye el tratamiento automatizado de la información, vale decir tratamiento de la información mediante ordenadores.

f).-INTELIGENCIA ARTIFICIAL.

TURING.- Consideraba que "Conducta Inteligente", era la capacidad de lograr en una máquina la eficiencia a nivel humano en cualquier actividad de tipo cognoscitivo. La prueba consistía en el interrogatorio de un ser humano a una computadora por medio de un teletipo: si el ser humano era incapaz de discernir si las preguntas habían sido respondidas por otro hombre o por una computadora, entonces se consideraba aprobada la prueba (Computer machinery and intelligence, " Journal Mind", 1950, vol. 59,p.433 a 460.

g).-ROBOTICA.

Denomínase así a la aplicación de robot en la toma de decisiones propias, por medio de la determinación de comportamientos adecuados en una situación dada, utilizando sensores físicos que le proporcionan la retroalimentación en base a la utilización de IA.

h).-REALIDAD VIRTUAL. (RV).

Dos Términos antagónicos como son realidad y virtual, son utilizados como una expresión por la Tecnología de la Información TI, para expresar la idea de algo que no existe en la realidad física, pero da la sensación de que existiera.

En el campo de lo virtual la computadora y las telecomunicaciones omiten lo físico, descorporizando y posibilitando alcanzar metas que son imposibles dentro de lo que es real.

La idea de los investigadores era encontrar un medio que posibilitaría la unión entre la mente humana y los dispositivos de computación que ellos denominaron "ambientes exploratorios de computadora".- Nicholas Negroponte, Richard Bolt. 1970.- Instituto de Massachussets.

i).-CRIPTOGRAFIA.

Denomínase Así a la herramienta más promisoria para lograr la seguridad y confiabilidad en las comunicaciones electrónicas y, de este modo, favorecer el pleno desarrollo del potencial de las redes abiertas.

La Criptografía nace como necesidad real de las redes de comunicación, las mismas que por su naturaleza técnica, al no tener una conexión física directa entre emisor y receptor que garanticen la confidencialidad de la información, se torna vulnerable y da lugar a la captación fácil, de la información.

j).-REDES.

Es el conjunto de computadoras interconectadas entre sí a los efectos de compartir recursos como: información, discos, impresoras, módems, etc.

I.2 DERECHO A LA INTIMIDAD

El derecho a la intimidad es entendido como "el poder o potestad de tener un domicilio particular, papeles privados, ejercer actividades, tener contactos personales y pensamientos que no trascienden a terceros, en virtud del interés personal de mantenerlos en reserva y la discreción de quien se entera de no hacerlos públicos cuando se trata de derechos privados o datos sensibles de las personas."(Pierini, p.237)

De esta manera, el derecho a la intimidad abarca el ámbito personal del individuo, quien tiene la facultad de tener un espacio en el que conserva datos e información que son solo de su incumbencia y que por tanto deben ser protegidos. Sin embargo, en la sociedad de hoy es muy difícil mantener una completa reserva acerca de los datos personales del individuo, puesto que las necesidades sociales y los avances tecnológicos han hecho que existan bancos de datos en los que se guarda información general sobre los usuarios de los distintos servicios y sistemas.

La Constitución Política del Ecuador al tratar el tema del derecho a la intimidad, estipula que:

"Art. 23 numeral 8 "Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el

nombre, la imagen y la voz de la persona." De igual forma, en el mismo Artículo, numeral 21 "El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a la salud y vida sexual, salvo para satisfacer necesidades de atención médica."

Al tratar el tema de la protección de datos personales es fundamental adentrarnos al derecho a la intimidad, puesto que "la protección de datos no ha sido imaginada para proteger a los datos per se, sino a su fundamento, que es la protección de una parte sustancial del derecho a la intimidad: la que se refiere a la información individual."(Ekmekdjian, p.5)

Es así como el art.9 de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, prescribe:

Art. 9 "Protección de datos: Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderán a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con

autorización del titular u orden de autoridad competente. . .)"

I.2.1 DOCTRINAS SOBRE EL DERECHO A LA INTIMIDAD

Es trascendental establecer que las distintas doctrinas sobre el derecho a la intimidad han ido evolucionando y ajustándose a los cambios de la época, es así como los cambios tecnológicos trajeron una revolución y un cambio decisivo en la concepción de este derecho. Esto se da por el hecho de que el desarrollo de la tecnología ha tenido una influencia directa en el fuero interno de las personas, por tanto el derecho a la intimidad debe ser observado y asimilado con relación a los efectos y consecuencias que traen los cambios en la sociedad y en las personas, consideradas como entes particulares.

El Derecho a la Intimidad tiene orígenes angloamericanos, fue definido por el juez Cooley como "the right to be let alone."(Ekmekdjian, p.8) y está orientado a proporcionar una estricta protección legal del individuo, contra la publicidad de datos personales o de actos personales que se ponen en conocimiento del público, pues esta es información que pertenece, únicamente, a la persona y por ende ésta es la única facultada para autorizar y decidir que se puede publicar o no.

Existen cuatro doctrinas que presentan al derecho a la intimidad desde sus inicios y su evolución en una era de cambio social constante.

La primera, plantea la presencia de un derecho general a la privacidad y en virtud de su existencia se abre la posibilidad a la protección jurídica en el caso de la violación de la vida privada, ocasionada por los distintos medios y vías de comunicación.

La segunda, evidencia que una de las características sustanciales del derecho a la intimidad es el control de la información, "en ella se lo define como el derecho de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y con qué extensión puede ser comunicada a terceros la información acerca de aquéllos." (Ekmekdjian, Miguel Angel, Corpus Data el Derecho a la Intimidad frente a la Revolución Informática, Editorial de Palma Buenos Aires, 1998, p.9)

Una tercera posición se sustenta en una formulación económica del derecho a la intimidad, la cual lo concibe como la suma de la difusión y retención de información en el contexto comercial y personal. Esta propuesta desnaturaliza el derecho a la privacidad, puesto que deja de lado los valores éticos, morales e individuales que conlleva este derecho.

La última teoría muestra una posición neutral en referencia al derecho a la intimidad, la cual "da cabida a las diferentes funciones de la protección legal del individuo en contextos diferentes de la sociedad automatizada: desde el procesamiento automático de información hasta la intercepción telefónica." (Ekmekdjian, p.10)

Dado esto, Estadella Yuste establece los puntos sobresalientes de la evolución de estos derechos:

1) Aunque la información personal puede tener un valor económico, no por ello deja de tener fundamentalmente valores personales (éticos). La información personal forma parte de la intimidad individual y se funda en el concepto de la autonomía individual para decidir, dentro de cierto límite, cuándo y qué información puede ser objeto de procesamiento automatizado.

2) La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente como consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a la comunidad toda, tanto nacional como internacional.

La idea de que la persona titular de los datos - el afectado - tiene interés, como parte de un grupo, en controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la primera etapa de leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual.

3) En algunos casos el tratamiento de datos automatizados se ha llegado a convertir en un arma estratégica de manipulación de conductas individuales.

4) La aplicación de avanzados métodos telemáticos a la información de carácter personal ha dejado de ser la excepción para convertirse en una rutina diaria; en

consecuencia, hay que tratar el tema como una realidad, y no como un problema hipotético. (Ekmekdjian,Miguel Angel, Corpus Data el Derecho a la Intimidad frente a la Revolución Informática, Editorial de Palma Buenos Aires, 1998, p.12)

Estadella Yuste plantea situaciones que forman parte de la realidad de hoy en día. Con las que nos hace concienciarnos sobre el hecho de que la automatización de la información, la informática, las nuevas tecnologías de la información y comunicación son realidades palpables que se manifiestan en nuestra vida diaria. Por tanto, como Estados responsables hay que tomar las medidas legales fundamentales, las que deben constituir los cimientos de esta sociedad de la información y comunicación.

La solución no es excluirnos de las innovaciones que trae la tecnología, la respuesta está en irnos adaptando, adecuadamente, a las nuevas necesidades que éstas generan. Con el fin de proporcionar a los ciudadanos los derechos y garantías establecidos en la Constitución, pero adaptados a las diferentes facetas, que estos cambios pueden traer.

CAPÍTULO

II

LA INFORMÁTICA Y LA

PROTECCIÓN DE DATOS

LA INFORMÁTICA Y LA PROTECCIÓN DE DATOS

"La irrupción de la informática en la sociedad ha replanteado la cuestión de la protección del derecho a la intimidad, en virtud del riesgo que para las personas implica la estructuración de grandes bancos de datos de carácter personal, y particularmente la potencialidad del entrecruzamiento de la información contenida en los mismos, lo que plantea la necesidad de elaborar un moderno concepto de protección del derecho a la intimidad, es decir, la necesidad de respuestas jurídicas que protejan los abusos en la manipulación de la información personal." (Pierini,1999: p.159)

El desarrollo tecnológico ha traído grandes ventajas para la sociedad, uno de los ámbitos en donde se observa una influencia más marcada es en el área de la informática, puesto que ha permitido la utilización del tiempo y de los recursos humanos de una forma más eficiente y eficaz, a través, de la inserción de medios mecánicos para la automatización de tareas (hardware) y la aplicación de programas específicos (software). Es así, como la informática abarca lo referente al estudio de los distintos sistemas de información, y la forma en que ésta va a ser generada, comunicada y compilada.

El desarrollo en el área tecnológica ha permitido crear ordenadores con gran capacidad para almacenar información. Si a esto adicionamos el punto del increíble avance en las comunicaciones; podemos

concluir que en la sociedad de hoy existen fuentes de datos, que están dispersas y que son accesibles a una gran cantidad de personas, a través, de la utilización de redes informáticas como es el caso de la Internet.

II.1.- BASES DE DATOS.

Para poder profundizar más, es importante tratar el tema de los bancos o bases de datos. Éstas no son un invento de la informática, no obstante adquieren una especial relevancia cuando añadimos el término informático. Lo que se da porque existen varias formas materiales de almacenar datos, pero éstas tienen un limitante que es el espacio.

Sin embargo al utilizar un soporte informático esto pierde importancia, puesto que estos mecanismos tienen una capacidad para almacenar información que sobrepasa los medios tradicionales es así como *"la cantidad de información que puede almacenar un disco compacto es equivalente a varias bibliotecas muy pobladas"* (Pierini, 1999: p.131)

Los datos pueden irse agrupando en bases o bancos de datos, que son archivos de datos almacenados en un ordenador, al cual podemos acceder de forma directa o por medio de la vía telemática. Un banco de datos de caracteriza por: *"a) El tratamiento de la información; b)El medio electrónico de ese tratamiento (hardware y software); c) La conjunción de esos datos con una finalidad o motivo propio."* (UICICH, 1999: p. 46)

Así, Gozaíni define a las bases de datos *como "el conjunto organizado de informaciones que han sido objeto de tratamiento o data mining que permite realizar entrecruzamientos y prospecciones para interpretar los datos almacenados."* (Gozaíni,2001: p.135)

Un banco de datos es un conjunto de datos estructurados, organizados y reagrupados por conjuntos homogéneos. Éstos para su funcionamiento deben considerar como referente a ciertos principios aplicables a este tipo de archivos, entre los que nombraremos: Principio de legalidad; Principio de finalidad, Principio de congruencia; Principio de corrección; y Principio de seguridad (técnica y lógica).

Por otro lado, las bases de datos poseen una clasificación, de acuerdo con ciertos criterios; entre los que podemos citar los siguientes:

a) ARCHIVOS PÚBLICOS Y PRIVADOS: Los archivos públicos constituyen registros que contienen información sobre las actividades del Estado, éstos pueden ser obtenidos por terceros, con la presentación de una solicitud. En algunos casos esta petición no es necesaria, así por ejemplo, en la página web del I. Municipio Metropolitano de Quito, basta con ingresar el nombre de la persona, para que aparezcan los bienes que se encuentran catastrados a su nombre; y no solo eso, sino que al insertar el apellido se encuentran los bienes catastrados a nombre de todas las personas que tienen ese apellido. De ahí, que

es necesario normar la protección de datos personales, con el fin de que esta información no sea expuesta con tal facilidad a terceros no interesados. En otra instancia, encontramos los archivos privados, que son aquellos que registran datos de personas físicas o jurídicas con una finalidad determinada, éstos no afectan a la intimidad en cuanto no permitan la identificación con la persona que es titular de la información contenida.

b) ARCHIVOS MANUALES E INFORMÁTICOS: Estos se clasifican según su modo de registro, puesto que la protección debe darse a los dos tipos de archivos, sin importar el mecanismo utilizado para su conservación.

c) ARCHIVOS DE SEGURIDAD DEL ESTADO: Son archivos que poseen información de personas físicas, y que generalmente están excluidos del hábeas data, en razón de que el Estado posee causas suficientes que justifican la reserva.

d) ARCHIVOS HISTÓRICOS: Es aquel que *"contiene intimidades de héroes y personajes de la vida y tradición de los pueblos, que se exponen al conocimiento público como una muestra de sus personalidades"* (Gozaíni,2001: p. 142)

e) ARCHIVOS PENALES: Son archivos que contiene información referente a los antecedentes penales de una persona, motivo por el cual el hábeas data no procede en estos casos.

f) ARCHIVOS CIENTÍFICOS O DE INVESTIGACIÓN: Son bases de datos generadas con fines de investigación, así en la generalidad de los casos el hábeas data se encuentra excluido; no obstante, cuando dentro de la investigación se mencionan a personas naturales con perfiles determinados, se debe establecer las medidas de seguridad correspondientes, que eviten una transferencia de estos datos sensibles.

g) LOS SERVICIOS ESTADÍSTICOS: Son archivos que contienen información procedente del relevamiento estadístico, el cual es realizado bajo los principios de reserva y confidencialidad; dicha información ha sido recolectada con el fin de establecer parámetros aplicables a la sociedad.

h) LOS BANCOS DE DATOS GENÉTICOS Y LOS BANCOS DE ÓRGANOS: Estos bancos de datos necesitan protección especial, puesto que manejan datos sensibles, que podrían afectar a la intimidad de un individuo, por lo que su procesamiento debe estar estrictamente regulado.

i) ARCHIVOS DE ENTIDADES FINANCIERAS: Trata sobre archivos que contienen datos personales obtenidos por medio de fichas, que llena el usuario con el fin de establecer una relación con esta institución. Esta información debería ser reservada y confidencial, mas existe un intercambio de ésta.

j) LOS ARCHIVOS FISCALES: Son archivos generados con la información que declaran los contribuyentes, bajo

los principios de confidencialidad y secreto. Estas bases de datos están destinadas a ejercer un control sobre el cumplimiento de las cargas públicas, por parte de los administrados.

k) EL REGISTRO ELECTORAL Y LAS FICHAS DE LOS PARTIDOS POLÍTICOS: Es una base de datos típica, que se requiere para ejercer el derecho a votar.

(Gozaíni, Oswaldo Alfredo "Hábeas Data Protección de Datos personales, Editorial Rubinzol - Culzoni, Buenos Aires, 2001).

II.2 TIPOS DE DATOS

Como hemos podido observar un banco o base de datos tiene como principal objetivo el almacenamiento de datos, para facilitar su acceso, registro e intercambio. Es así, como estos datos pueden clasificarse de acuerdo a distintos parámetros, entre los que encontramos:

1.- POR LA IDENTIFICACIÓN DEL TITULAR DEL DATO:

a) NOMINATIVO: Es el dato que pertenece a una persona física conocida e identificada. Al respecto Uicich manifiesta que: *"Dato nominativo: Es aquel que está referido a una persona determinada. Se lo divide conforme a su forma de acceso a la identificación de la persona, así encontramos: 1. Directos: cuando identifica al individuo sin necesidad de proceso alguno; 2. Indirectos: cuando permite la identificación pero no lo identifica en forma*

directa sino agrupando datos. A su vez el dato nominativo puede clasificarse en 1. Dato nominativo sensible: Aquel que afecta o puede afectar a la intimidad. Dato nominativo no sensible: Es aquel que si bien es personal, está destinado a ser público, como el número de cédula de ciudadanía."(UICICH,1999: p. 47)

De esto se desprende, que la protección de datos personales adquiere relevancia cuando nos referimos a los datos nominativos, en especial a los sensibles. Puesto que éstos poseen información capáz de identificar a una determinada persona, de ahí que la difusión sin control de esta información se puede convertir en un foco para la transgresión del derecho a la intimidad.

b) INNOMINATIVO O ANÓNIMO: Es el dato estadístico o general que no personaliza ni permite la personalización, puesto que la información contenida no se dirige a identificar a la persona, sino que trata sobre sus actividades.

2.- POR LA CONFIDENCIALIDAD DE LA INFORMACIÓN:

a) DATOS QUE NO AFECTEN A LA SENSIBILIDAD DE LAS PERSONAS: Es aquella información irrelevante, que por su contenido no afecta a la intimidad de los individuos

b) DATOS QUE AFECTAN A LA SENSIBILIDAD DE LAS PERSONAS: *"Son los que de difundirse ponen en conocimiento de quien los conoce datos de contenido*

privado que, salvo manifestación expresa del afectado, socavan la intimidad de las personas" (Gozaíni,2001: p.233). Dentro de éstos se encuentran los datos sensibles, que son aquellos que contienen información sobre la ideología, religión, creencias, origen racial, salud y vida sexual del individuo, de ahí que su protección sea una necesidad inminente.

3.- POR LA MAYOR O MENOR COMPLEJIDAD PARA LOGRAR EL DATO SE CLASIFICAN EN:

a) DATOS PÚBLICOS O FÁCILMENTE CONOCIDOS: son aquellos que se encuentran en lugares públicos de fácil acceso, por lo que su disponibilidad la tiene cualquier interesado.

b) DATOS PRIVADOS, SECRETOS Y CONFIDENCIALES: El privado es aquel que es conservado por el individuo en la reserva de su intimidad. El secreto es aquel que implica el ocultamiento, para evitar que el dato salga de la esfera personal. El dato confidencial es aquel que por su grado de sensibilidad, no puede ser transmitido a terceros.

4.- POR LA SUBJETIVIDAD O PERTENENCIA DEL DATO:

a) DATOS PERSONALES EXISTENCIALES: *"Se denominan a los datos que se relacionan con definidores de la personalidad tales como natalicio, lugar de origen, estado civil, domicilio actual y profesional, entre otros."* (Gozaíni,2001: p.240). Heredero Higueras manifiesta que: *"Estos constituyen una masa de datos*

que no tienen carácter personal cuando no puedan ser asociados a personas determinadas o determinables."

Este es un punto de gran interés, puesto que puede ser que existan datos referentes a la intimidad de la persona, pero mientras ellos no puedan asociarse ni combinarse, con otros datos, que posibiliten la determinación del individuo, entonces esta información no posee la calidad de dato personal. Por tanto, surge el tema de la capacidad de interconexión de datos.

a) DATOS PERSONALES NO EXISTENCIALES: Son aquellos que se refieren al patrimonio económico de la persona.

POR EL SECRETO QUE GUARDAN:

Este es un tipo de datos que se refiere al secreto que debe mantener la persona que los guarda, y que generalmente está vinculado a su profesión.

Al hablar de la protección de datos personales nos centraremos en el tema específico de los datos personales nominativos, y especialmente en los datos personales nominativos sensibles, pues son éstos los que se encuentran íntimamente relacionado con el derecho a la intimidad de las personas. Por tanto, se debe establecer una normativa y mecanismos de control que salvaguarden esta información.

CAPÍTULO

III

TRATAMIENTO DE DATOS

PERSONALES PROCESADOS

EN MEDIOS ELECTRÓNICOS

TRATAMIENTO DE DATOS PERSONALES PROCESADOS EN MEDIOS ELECTRÓNICOS

Al abordar el tratamiento de datos personales, en medios electrónicos, nos referimos a los distintos procedimientos adoptados para la recopilación, conservación, ordenación, archivo, modificación, actualización, destrucción, distribución, y demás actividades que involucra el procesamiento de los datos personales. Al respecto, distintas legislaciones han establecido mecanismos para brindar protección a la intimidad de las personas, ante los avances tecnológicos e informáticos que día a día forman parte de nuestra vida.

El Tribunal Constitucional de Alemania señala que: *"no serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él"* (Gozaíni, 2001: p.64) Este criterio del Tribunal manifiesta de forma clara y precisa el derecho de las personas a autorizar expresamente cualquier actividad que involucre el procesamiento de datos personales, especialmente, en lo relacionado con la difusión y transferencia de éstos.

Al tratar este tema, Ana Isabel Herrán manifiesta que: *"Hoy nadie duda de que la vida privada de la persona es un bien que debe respetarse, porque el ataque a la misma es susceptible de causar un daño*

irreparable a la persona en una sociedad como la actual, cuyo único límite al almacenamiento y tratamiento de datos personales es el que procede de la imaginación humana. Información relativa al ocio, a los comercios o a la educación de los hijos, así como a las actividades profesionales no son inocuas en nuestro desarrollo personal y en la honorabilidad o imagen que se ofrece al exterior, por lo que oportunamente entrelazadas y almacenadas "dicen" mucho de cada individuo y de su personalidad; inmiscuirse en ellas, para conocerlas y tratarlas sin consentimiento, representa un peligro del que se debe ser consciente si se quiere una sociedad libre y en igualdad de oportunidades. Sentir que constantemente se está siendo observado, seguro de que la totalidad de las acciones serán "registradas", impide el derecho a manifestarse en una sociedad con libertad y dificulta el libre desarrollo de la personalidad. Habida cuenta de los nuevos peligros y amenazas que el tratamiento informático trae consigo, se sugiere una conceptuación del derecho a la autodeterminación informativa a través de una extensión de su protección frente al uso ilícito o abusivo de la informática a cualquier información personal que represente una amenaza a la persona en "manos de terceros"; la interceptación no consentida de la información debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información" (Herrán Ortiz, 1999: p.105)

Esta opinión muestra la forma en que los datos personales constituyen parte esencial del individuo. De esta manera, se expone cómo el tratamiento que se dé a esta información, dentro del ordenamiento jurídico,

puede afectar a la persona en su desarrollo como individuo y como ente social. Se desprende el efecto que posee la protección de datos personales a nivel de la comunidad, ya que las garantías legales que se proporcione a esta información, son esenciales para establecer los parámetros dentro de los que se manejará y participará la sociedad.

Por otro lado, El Tribunal Constitucional español establece que: "*el incremento de los medios técnicos de tratamiento de la información puede propiciar la invasión de la esfera privada, haciéndose necesaria la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en prácticas a través de cualquier instrumento que produzca tal efecto, y a incrementar las facultades de conocimiento y control que se otorguen al ciudadano para salvaguardar el núcleo esencial de su derecho (...) Las normas autorizatorias de recogida de datos, incluso con fines legítimos y contenido aparentemente neutro, deben incluir garantías adecuadas frente a su uso potencialmente invasor de la vida privada, por lo que si no lo hacen pueden y deben considerarse vulneradoras de la intimidad*" (TC, sentencia del 9-5-94) (Gozaíni, p. 60)

El fallo del Tribunal señala que si bien es necesaria la existencia de normas dirigidas, especialmente, a la protección de datos personales, éstas no deben abarcar, únicamente, los principios y parámetros de protección. De tal manera, que se debe incorporar a esta normativa mecanismos prácticos que

brinden una verdadera garantía a los titulares de esta información.

Este es el criterio de un Tribunal perteneciente a un Estado, que hace algunos años ya posee una normativa sobre protección de datos personales. Entonces, surge una interrogante ¿Cómo se protege el derecho a la intimidad en naciones como la ecuatoriana, en la que no existe ni siquiera un cuerpo legal destinado, exclusivamente, a salvaguardar los datos personales?

III.1 TRATAMIENTO DIRECTO, INTERCONECTADO O POR TERCEROS

La protección de los datos personales de los individuos se encuentra, íntimamente, relacionada con el derecho a la intimidad. De ahí, que su tratamiento es fundamental, para evitar la transgresión de derechos tanto individuales como de terceros. Por este motivo los archivos y bases de datos deben guardar determinados estándares, que brinden las suficientes garantías de seguridad y confidencialidad sobre la información proporcionada por las personas.

Es trascendental determinar el hecho de que para que se dé lugar a una efectiva protección de los datos personales, se necesita identificar las fuentes y la localización de los bancos de datos. De esta manera, los datos nominales obtenidos de forma directa son aquellos que la persona entrega de forma voluntaria; mientras que los datos nominativos indirectos son aquellos que se obtienen ya sea por la interconexión o por trabajos realizados por terceros.

El tratamiento directo de los datos personales, es aquel en el que, únicamente, intervienen el titular de los datos y la persona encargada del archivo o de la recopilación, dado que se toman directamente los datos del individuo.

El tratamiento interconectado es aquel en el que se produce un intercambio de la información contenida en las bases de datos, con el objetivo de encontrar un perfil, en el que se asienta un mercado para determinado producto. Así, por ejemplo si una base de datos contiene registros sobre el nivel de consumo mensual con tarjeta de crédito y los lugares de consumo; y otra base de datos posee información sobre clientes frecuentes de restaurantes; entonces se podrán fusionar y encontrar un perfil para poner a disposición de estos clientes un restaurante de alto nivel, que satisfaga sus expectativas y necesidades sociales.

El tratamiento de datos por terceros es un encargo en el que el agente autorizado delega a otro la recopilación de datos, adquiriendo este segundo las responsabilidades de secreto y confidencialidad; mas por el hecho de que el titular de los datos no lo ha autorizado de forma expresa, este tercero no puede utilizar la información y menos aún difundirla. *"La diferencia con la interconexión está en que no es este archivo el que ha tomado y guardado los datos, ni participa con el fichero original en el procesamiento de la información."* (Gozaíni,2001: p.284)

En España se ha establecido que: *"cuando los datos de carácter personal no hayan sido recabados del*

interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o de su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido del tratamiento y de la procedencia de los datos". Esto no se requiere *"...cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten"* (Gozaíni, 2001: p. 284)

De tal manera, se puede establecer que el titular de los datos tiene el derecho a ser informado en forma exacta y expresa cuando sus datos personales vayan a ser difundidos. Por cuanto, la persona tiene el derecho para permitir que sus datos sean compartidos o no, motivo por el cual tendrá la facultad de solicitar que se le informe sobre los fines para los que será transmitida la información, el responsable del procesamiento y el procesamiento en sí. Por razones obvias esto rige cuando los datos son de tal relevancia

que permiten la identificación del individuo, y no son de libre acceso público.

III.2 MODALIDADES DEL TRATAMIENTO DE DATOS

Existe una gran variedad de bases de datos, las cuales adquieren sus puntos distintivos dependiendo del fin para el cual han sido creadas. De tal manera, el interés que las define es el que establece los parámetros dentro de los que se llevará a cabo su funcionamiento. Por tanto, realizaremos un estudio sobre las modalidades del tratamiento de datos, dependiendo del área de manejo.

III.2.A INTERNET

La Internet es un fenómeno tecnológico de nuestra época, en razón de que constituye un medio de comunicación que ha roto las barreras del espacio y del tiempo. De esta forma, esta inmensa red permite la interrelación con miles de redes existentes en el mundo, permitiendo de esta manera el intercambio de comunicación masiva entre los ordenadores que se encuentran vinculados.

La Internet puede ser considerada como la mayor base de datos a nivel mundial. Toda la información que contiene puede ser consultada simultáneamente por todos los usuarios. Una vez que una información entra a la red es imposible detenerla, y aunque posteriormente intente ser retirada por su titular, una impensable cantidad de copias pueden estar circulando de forma

ingobernable o haber ingresado a un sinnúmero de bases de datos.

Al estar los datos personales en la Internet el derecho a la intimidad se ve afectado, puesto que sin necesidad de la debida autorización del usuario, otras personas pueden tener acceso a información que corresponde al fuero íntimo de la persona.

Es así, como se ha dado origen a un nuevo espacio, el ciberespacio, el cual se caracteriza, esencialmente, por su intangibilidad, lo que le ha dado una gran flexibilidad de regulación. De tal forma, nos vemos inmersos en una aldea global que se encuentra conectada y comunicada por la tecnología. En la cual surgen muchos interrogantes, dentro de los que los relevantes para nuestro estudio serían: ¿ Cómo protejo mi intimidad en Internet? ¿Cuál es el tratamiento que se da a los datos personales en Internet? Para poder resolverlos es fundamental establecer los puntos que abarca la Internet.

III.2.A.a) RECURSOS DE INTERNET

Dentro de los servicios que proporciona la red podemos identificar:

El correo electrónico; que significa transacciones comerciales electrónicas.

El file transfer protocol (FTP), que consiste en la interconexión entre ordenadores;

Telnet, que permite el uso de programas contenidos en otros ordenadores;

Gopher, cuya función se enfoca en la localización de bases de datos y programas que se encuentren en la red;

Usenet, el cual facilita la creación de foros virtuales en los que personas pueden tratar distintos temas de interés y,

El hyper text transfer protocol (HTTP), que es el lenguaje técnico que usa la red.

Como se puede observar la Internet, actualmente, está destinada a facilitar el intercambio de información, lo cual no tiene límites, solo los de la imaginación humana. Puesto que provee de herramientas que permiten ingresar y obtener información de un sinnúmero de temas, sin que exista un control sobre ésta.

III.2.A.b) CÓDIGOS DE CONDUCTA

Existe una ausencia de normas sobre este tema, de tal manera solo se han realizado posibles proyectos a seguir. Por otro lado, se ha encontrado una gran dificultad para homogeneizar las legislaciones nacionales sobre este tema. Es así como se han fijado códigos de conducta, los que contienen los principios y referentes guías para el manejo de esta actividad.

El objetivo es generar una conciencia colectiva que permita brindar los estándares mínimos para la

protección de la intimidad en Internet, dejando de lado la autorregulación de la red. El fin es que el titular de los datos se encuentre debidamente informado sobre la finalidad que se darán a los datos recopilados.

Afirma Rodotá que *"la Federal Trade Commission (FTC) realizó en febrero de 1998 un estudio sobre 1400 empresas, observando que el 85% de ellas recopilaba datos personales con regularidad; solo el 14% ofrecía información al afectado sobre el destino que se daba a esos datos, y apenas un 2% había adoptado políticas de protección a la intimidad."* (Gozaíni,2001: p. 288)

Por esta razón es muy importante que los usuarios, antes de ingresar sus datos, revisen las políticas de confidencialidad y seguridad de la página web en cuestión. Pues, únicamente, esta operación proporcionará las bases para establecer el destino de dichos datos y los procedimientos utilizados dentro del procesamiento de esa información.

III.2.A.c) ¿CÓMO PROTEGER LA INTIMIDAD EN INTERNET?

Al tratar el tema Gozaíni establece que: *"La experiencia mundial parece establecer una triple escala en la problemática.*

A Internet se le asignan códigos éticos. Un marco que pretende evitar el uso y abuso de informaciones sensibles.

A los sitios en la red, que pueden ser los bancos de datos en potencia, se les requiere una suerte de

certificación sobre motivos de creación, finalidades previstas, destino de la información y control que sobre los datos procesados se tiene.

El tercer modelo o escalón diseñado pretende incluir una red mundial que garantice la calidad de las direcciones de Internet en vista a ganar la confianza del usuario.

Microsoft afirma que Internet es una herramienta sorprendente que tiene la capacidad de cambiar la forma de vida. Por eso, en sus sitios suele presentar una "Declaración de privacidad", donde establece varios principios:

1)La información del perfil personal solo se utiliza para realizar estadísticas demográficas y para mostrar anuncios personalizados. Los datos se guardan sin compartirlos con otras empresas.

2) Solo se envía la información solicitada; 3)Se permite el derecho de acceso permanente para el usuario que considere que la empresa no respeta sus principios de privacidad."(Gozaíni,2001: p.289)

Es de gran importancia que los usuarios de Internet y de páginas Web, en las que se recopilan datos personales, nos conciencemos sobre la importancia de este tema. El objetivo de esto radica en que como usuarios exijamos la adopción y respeto de los mencionado códigos de conducta. De tal manera, que las personas que posean una página Web contemplen dentro del contenido de dicha página, una declaración de

privacidad, mecanismos para verificar el uso y fines de la recolección, direcciones seguras, y demás mecanismos necesarios para proporcionar la confianza requerida a los usuarios, para que puedan ser partícipes activos dentro del desarrollo de la sociedad de la información.

III.2.B COMERCIO ELECTRÓNICO

El Comercio Electrónico "*en su acepción más común hace referencia a las transacciones comerciales electrónicas, es decir, a la compraventa de bienes o prestación de servicios, así como a las negociaciones previas y otras actividades ulteriores relacionadas con los contactos, especialmente, las relativas a la ejecución contractual, efectuadas a través de los mecanismos que proporcionan las nuevas tecnologías de la comunicación*" (Martínez Nadal, internet: p. 27)

Al realizar este tipo de actividades de intercambio comercial, a través, de redes informáticas; las partes de forma voluntaria proporcionan datos personales; los cuales al ingresar a una red abierta, quedan al alcance de terceros. Es así, como se puede apreciar que la utilización de este tipo de redes abiertas da lugar a la formación de un canal en el que el intercambio, acceso, tratamiento y cesión de datos personales a terceros es mucho más fácil y viable, con lo que se deja de lado que estos datos fueron obtenidos para cumplir un fin específico y no para constituirse en una fuente de información de terceros, cuyas intenciones desconocemos.

Dentro de los peligros más evidentes, contra la intimidad de las personas, que se presentan en el comercio electrónico encontramos:

1.- El rastro del dinero electrónico, generalmente, el pago en las transacciones electrónicas se realiza, a través, de tarjetas de crédito; motivo por el que el comprador tiene que ingresar sus datos personales como nombre, dirección, número de tarjeta; y al entregar esta información es muy posible que se vincule la identidad del usuario con los productos comprados, creándose perfiles de mercado.

2.- Inseguridad de las transacciones electrónicas, lo cual se presenta por el temor de que los datos suministrados para la realización de las transacciones electrónicas sean intervenidos por un tercero que no es el vendedor; por otro lado, el vendedor debe tener constancia de que el comprador es en realidad quien dice ser.

3.- Envío de publicidad no deseada o *spam,* muchas veces recibimos publicidad de productos que no hemos solicitado, lo que implica que ha existido un intercambio, cesión o interceptación de los datos personales proporcionados

Las operaciones de comercio electrónico dan origen a relaciones entre empresas, y, entre empresas y consumidores; motivo por el que su naturaleza se delimita a la esfera de lo privado. La Ley Orgánica de Protección de Datos de Carácter Personal de España (LOPDAT), regula el tratamiento de ficheros tanto de

naturaleza pública como privada, los cuales comparten normas comunes, no obstante, para el análisis de este tema nos centraremos en los de titularidad privada.

En virtud de la relación jurídica establecida por las actividades de comercio electrónico, existen por un lado, individuos que han ingresado sus datos personales en un fichero, a éstos la ley los denomina como afectado o interesado, y los define como *"persona física titular de los datos que sean objeto de tratamiento"* (Gozaíni,2001: p.472).

En otra instancia, se encuentra el responsable del fichero, quien es la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento" (Gozaíni,2001: p.472). Este concepto posee un carácter significativo dentro de la normativa para la protección de datos personales, en razón de que debe estar especificado el agente responsable del procesamiento de esta información, ya que existen responsabilidades directas que se relacionan con el ejercicio de sus funciones.

El objetivo de la Ley es brindar una protección al titular de los datos personales, sobre el tratamiento que se dará a esta información, no obstante, esta protección no se da en forma absoluta. Puesto que el titular al proporcionar libre y voluntariamente sus datos, se somete a un riesgo que consiste en que sus datos sean distribuidos a terceros, lo que puede afectar su privacidad; sin embargo, la transacción le representa beneficios mayores, razón por la que decide

realizarla. De esta manera, la Ley tiende a conciliar estas posturas, dando así una protección equilibrada.

En este punto cabe recalcar la importancia de la determinación del responsable del tratamiento de los ficheros. Puesto que sobre este agente recaerán obligaciones y derechos, aspectos de vital importancia para este tema. Así, éste es el encargo de tomar las medidas técnicas y administrativas, que garanticen la seguridad y confidencialidad de los datos contenidos en el archivo.

Otro aspecto relevante es la definición del destino que se dará a los datos procesados. Con el objetivo de que su uso se mantenga circunscripto a los parámetros establecidos, por las partes, en el contrato. Dentro de este apéndice es fundamental fijar la pertinencia de los datos recopilados, en función del objetivo que se busca con ellos.

III.2.B.a. CÓDIGOS DE CONDUCTA

El titular de los datos, al realizar transacciones electrónicas, deberá exigir que se respeten como mínimos los siguientes códigos de conducta:

1. Ser informado de la identidad y ubicación de las entidades que ofrecen comercio electrónico y validar estos datos.

2. Obtener productos y servicios auténticos especificados en las ofertas.

3. Disponer de un mecanismo de corrección de los problemas derivados de las operaciones comerciales.

4. Recibir la formación adecuada sobre sus derechos en el ciberespacio.

Con sus datos personales el individuo podrá:

1. Disfrutar de la oportunidad y la habilitación individual para navegar y efectuar las operaciones comerciales en el anonimato.

2. Ser informado desde el comienzo sobre la finalidad y las posteriores utilizaciones y divulgaciones de los datos personales recopilados por los usuarios de éstos.

3. Exigir que la información personal recogida sea exacta y se almacene en condiciones de seguridad.

4. Tener derecho de acceso y de corregir los datos inexactos.

5. Optar por la exclusión voluntaria.

6. Solicitar que los datos almacenados de niños se sometan a la autorización y control de los padres.

(Gozaíni, 2001: p. 300)

III.2.C DATOS PERSONALES EN LAS TELECOMUNICACIONES

La sociedad de la información y comunicación ha traído innovaciones en las comunicaciones electrónicas. De tal manera, el surgimiento de las líneas digitales ha proporcionado nuevos servicios, así como cambios en el tratamiento de datos personales provistos por los usuarios.

La Comunidad Económica Europea, es una de las que posee una Normativa avanzada con respecto a este tema, de ahí que, con fecha 12 de julio de 2002 se aprobó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, la cual deroga a la directiva 97/66/CE, que contempla el tema de tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, para lo cual se ha previsto un plazo de transposición fijado para el 31 de octubre de 2003. Si bien las Directivas no constituyen auto aplicables para los países que conforman la Unión Europea; establecen estándares de protección, que están orientados a homogeneizar las legislaciones nacionales, hecho que acarrearía sanciones para los Estados miembros, en caso de que éstos no adopten las normas contempladas en las Directivas.

La Directiva antes mencionada, al igual que las normas vigentes, están orientadas a proteger la intimidad, para lo cual se han establecido mecanismos de protección de este derecho, con relación a los datos personales que son objeto de tratamiento, así como de los derechos que le asisten al usuario del servicio:

Leire Sainz de la Maza, al realizar un estudio sobre la esta nueva Directiva establece los datos sobre el tráfico, serán definidos como aquellos que se tratan con el fin de lograr la conducción de una comunicación, a través, de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.

El Real Decreto 1736/1988, que desarrolla el Título III de la Ley General de Telecomunicaciones establece una lista, en la que determina cuales son los datos que podrán ser tratados a efectos de control del tráfico y facturación.

a) El número o la identificación del abonado.

b) La dirección del abonado y el tipo de equipo terminal empleado para las llamadas.

c) El número total de unidades que deben facturarse durante el ejercicio contable.

d) El número del abonado que recibe la llamada.

e) El tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos.

f) La fecha de la llamada o del servicio.

g) Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.

Los mismos, una vez que han sido utilizados para el fin para el que fueron almacenados y tratados (transmisión de una comunicación, facturación de los abonados, pagos de las interconexiones) deberán eliminarse o hacerse anónimos. Pudiendo tratarse y almacenarse únicamente por el plazo durante el cual pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable.

En todo momento el abonado o usuario del servicio deberá poder conocer qué datos de tráfico están siendo tratados por el proveedor del servicio. En el caso de que el proveedor decidiera tratar los mismos con fines de promoción comercial, respecto de servicios relacionados que sean prestados por él mismo, se requerirá el previo consentimiento del abonado o usuario.

Siendo preciso a estos efectos, que el proveedor del servicio dirija una comunicación a sus abonados donde se les informe del objeto de tratamiento de sus datos, con el fin de que estos consientan el mismo, sin necesidad de que sea expreso ya que una no contestación se considerará que no se opone y por lo tanto el abonado dará su consentimiento para efectos prácticos.

Datos de localización, constituyen un nuevo concepto introducido por la nueva directiva, entendiendo por los mismos *"aquellos que indiquen la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponibles para el público"*, éstos podrán ser tratados previo consentimiento (cuando los datos no fueran

anónimos) del usuario o abonado, para la prestación de servicios de valor añadido.

Siguiendo en esta misma línea, debemos hablar de los datos que figuran en las facturas desglosadas, donde el abonado puede encontrar de forma detallada cuáles son los números de teléfono a los que se han efectuado las llamadas, día y hora de comienzo, duración y tipo de la llamada, así como el volumen de datos transmitidos.

Sin duda el uso de este modelo de facturas además de ofrecer al abonado información a efectos de confirmación de las tarifas aplicadas, puede constituir un ataque al derecho a la intimidad de los usuarios que efectúan las llamadas y de los abonados que las reciben, debido a la información que en éstas se detalla. Es por ello que se hace preciso ofrecer modalidades alternativas de comunicación de las facturas o medios de pago que garanticen el anonimato, como podrían ser la omisión de un determinado número de cifras en la factura de los números a los que se ha llamado o la no aparición en la factura de los números a los que se llama, cuando el pago se haga con tarjeta de crédito, como mecanismos de garantía de la utilización anónima o estrictamente privada del servicio.

En todo caso, será el propio abonado quien decida renunciar al envío de este modelo de facturas. Por otro lado, tenemos los servicios de identificación de la línea de origen y de la línea conectada que pueden prestarse, a través, de líneas digitales, aquí existe

una clara confrontación entre el derecho de quien recibe la llamada de saber quién le llama, como el derecho de quien efectúa la misma a guardar su anonimato, en este mismo sentido también se reconoce el derecho a rechazar llamadas entrantes de usuarios o abonados que hayan impedido la presentación de la identificación de la línea de origen.

Existe otro tipo de servicio, ofrecido cada vez más por algunos operadores, como es el registro de llamadas, en donde quedan almacenadas las llamadas que el abonado ha recibido cuando éste se encontraba ausente. Ello trae de nuevo la disyuntiva entre el derecho a la información y el derecho a la intimidad.

Son servicios que el abonado podrá solicitar a su proveedor de forma gratuita y éste tendrá el deber de proporcionárselos siempre y cuando no existan motivos que impidan esta posibilidad, como es el caso de llamadas maliciosas, servicios de urgencia, entre otros.

Donde por razones obvias se hace necesario conocer el origen de la llamada y no será preciso el consentimiento del abonado para poder tener acceso a esta información de identificación de la llamada entrante.

Las guías de abonados, constituyen una fuente de acceso público de acuerdo con el art.3.j) de la LOPD, donde constan datos del abonado como son el nombre, apellidos, dirección completa de su domicilio(los estrictamente necesarios para identificar al abonado),

sin embargo se requiere que el abonado sea informado previamente a su inclusión en la correspondiente guía, de qué datos personales van a constar en dichas guías tanto impresas como electrónicas para su posterior consulta por cualquier ciudadano, así como la finalidad y posteriores usos que sobre las mismas se puedan realizar.

Esta obligación a los proveedores de los servicios no será de aplicación respecto de las ediciones de guías ya producidas o puestas en el mercado con anterioridad a la entrada en vigor de las disposiciones que desarrollen la Directiva, aprobada al efecto de la privacidad y comunicaciones electrónicas. En todo caso el abonado podrá decidir cuales de estos datos desea que sean públicos en las guías.

Se abre la posibilidad de que las operadoras incluyan otros datos del abonado en las guías, pero en estos casos siempre previo consentimiento expreso del abonado.

El hecho de que los datos que constan en las guías telefónicas sean calificados como de acceso público y no precisen de consentimiento previo del abonado para su captación, provoca que en ocasiones puedan ser utilizados con fines de venta directa por distintas empresas, de ahí que al objeto de evitar el envío de publicidad no deseada, los abonados podrán exigir a los operadores entre otras; que se les excluya de las guías, que se omita parcialmente su dirección o bien podrán darse de alta en listas Robinson obligando de esta manera a las compañías de venta directa a darles

de baja de sus ficheros, indicando que sus datos personales no podrán utilizarse para fines de venta directa. Los operadores requeridos deberán cumplir lo dispuesto, sin que ello conlleve coste alguno para los abonados y sin que se vean limitados sus derechos como abonados de la línea.

Hasta ahora, se ha hablado de las distintas garantías que la Ley ofrece al objeto de salvaguardar la integridad del derecho a la intimidad de los abonados, pero también ha de señalarse que no nos encontramos ante un derecho absoluto e ilimitado, dado que en ocasiones podrá verse restringido por los gobiernos de los distintos estados, amparándose en el paraguas de la salvaguarda de la seguridad nacional. De esta forma se encuentra reflejado en la legislación española y normativa comunitaria.

A pesar de que la Directiva 97/66/CE, en su artículo 5, reconoce el derecho a la confidencialidad de las comunicaciones realizadas a través de redes públicas de telecomunicación y de los servicios de telecomunicaciones accesibles al público, sin que esté permitido la escucha, grabación, almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y de los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados. Sin embargo, sí se autoriza el acceso a los mismos por personas que estén autorizadas legalmente (en este mismo sentido se pronuncia el artículo 14 de la presente directiva fijando la posibilidad de que, los Estados miembros podrán adoptar medidas legales para

limitar el alcance de las obligaciones y derechos, cuando estas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicación a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE).Igualmente la Directiva 2002/58/CE se mantiene en idéntica posición.

Directamente relacionados con estos aspectos, existe un conjunto de documentos redactados en el seno del Consejo de la Unión Europea que amparan estas actuaciones de los Estados, permitiendo a los cuerpos de seguridad y policía de los distintos Estados efectuar interceptaciones en todo tipo de comunicaciones, sin que en ningún momento se concrete quien será la autoridad que facultará dichas intervenciones.

Los mismos se conocen como ENFOPOL, el primero fue la Resolución del Consejo de 17 de enero de 1995 sobre interceptación legal de las comunicaciones, en la misma se detallaban las obligaciones de las operadoras de telefonía para adoptar sus máquinas y de esta forma poder facilitar el acceso por parte de agencias y cuerpos de seguridad nacionales a las comunicaciones, los clientes y usuarios de las operadoras. Revisiones posteriores del documento en 1999 (Enfopol 98 y 99) extienden esta obligación a los operadores de Internet y GSM.

La redacción y aprobación de estos documentos, fueron precedidas de la calificación de los mismos como clase A, es decir, no requieren de previa consulta pública en el Parlamento Europeo para su aprobación, lo que sin duda muestra la falta de trasparencia con que se pretende tratar el tema.

Se considera interesante citar alguno de los artículos que componen estas Resoluciones, y de esta manera poder comprobar el alcance de las interceptaciones de las que podemos ser objeto por los Estados:

1. "Las autoridades competentes requieren tener acceso a todas las telecomunicaciones transmitidas o recibidas a través del número telefónico u otro código del servicio de telecomunicaciones interceptado que utilice el sujeto de la interceptación"

2. "Las autoridades competentes necesitan tener acceso a los siguientes datos relativos a las conexiones:
   Datos de tráfico (Señal de entrada, número de abonado al que va dirigida la llamada de salida, incluso si no llega a establecerse la conexión, número del abonado que realiza la llamada de entrada, inicio, final y duración de la conexión.....)"

3. "En el caso de abonados de servicios de telefonía móvil, las autoridades competentes

requieren informaciones lo más exactas posibles sobre la situación geográfica dentro de la red."

4. "Las autoridades competentes necesitan disponer de datos sobre los servicios específicos utilizados por el sujeto objeto de interceptación y sobre los parámetros técnicos de estos tipos de comunicación."

5. "Las autoridades competentes necesitan que las medidas de interceptación se efectúen de manera que ni el sujeto de la interceptación ni ninguna otra persona no autorizada puedan tener conocimiento de las modificaciones efectuadas para llevar a cabo la orden de interceptación. En particular, el servicio no debe dar ningún indicio de alteración al sujeto objeto de una orden de interceptación."

No obstante, el control de los gobiernos no se limita a esto;así, en primera instancia se encuentra el art.52 de la Ley General de Telecomunicaciones, que a pesar de reconocer la facultad de poder utilizar sistemas de cifrado en las comunicaciones para salvaguardar la integridad y confidencialidad de las mismas, igualmente, abría la posibilidad de que se establezca la obligación tanto para los fabricantes que incorporaran el cifrado en sus equipos o aparatos, como a los operadores que lo incluyeran en las redes o dentro de los servicios que ofrecían y, en su caso, a los usuarios que los emplearan en sus comunicaciones de notificar a la Administración General del Estado u organismo público los algoritmos o cualquier

procedimiento de cifrado utilizado, a efectos de control de dichas comunicaciones.

El reciente Proyecto de Ley General de Telecomunicaciones en su art.36.2 hace extensible la notificación a las propias claves de cifrado. Este intento de control absoluto de todas las comunicaciones, no podía quedar sin respuesta, de ahí, que gracias a campañas como las iniciadas por la Asociación de Internautas (AI), se haya conseguido que por medio de una enmienda el Gobierno haya rectificado y procedido a suprimir el polémico artículo (36.2). Consiguiendo de esta forma que de momento el mismo no sea conocido.

Entonces, cabe la pregunta dónde se encuentra el límite a la actuación de la Administración frente al derecho a la intimidad, es preciso que se establezcan garantías legales ante estas actuaciones, las cuales deberían estar siempre amparadas por una resolución judicial. Es preciso entender estas actuaciones como algo realmente excepcional, debiendo proteger a los ciudadanos frente a intromisiones injustificadas de los Estados en sus vidas privadas.

CAPÍTULO

IV

EL HÁBEAS DATA: UN INSTRUMENTO INSUFICIENTE PARA LA PROTECCIÓN DE DATOS PERSONALES

EL HÁBEAS DATA: UN INSTRUMENTO INSUFICIENTE PARA LA PROTECCIÓN DE DATOS PERSONALES

IV.1 EL HÁBEAS DATA

Pérez Luño manifiesta que *"El hábeas data constituye, en suma, un cause procesal para salvaguardar la libertad de la persona en la esfera de la informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación"* (Pérez Luño,1991: p.174)

La Constitución Política del Ecuador concibe al Hábeas Data como una garantía, así en su art. 94 estipula que: *"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en las entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización (...)"*

Dentro de los fallos de la Primera Sala de lo Contencioso Administrativo de la provincia de Córdoba - Argentina, se encuentra un pronunciamiento en el que se establece que: *"La acción de hábeas data es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su*

supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación. Esta información debe referirse con cuestiones relacionadas con la intimidad, no pudiendo utilizarse por terceros sin derecho a hacerlo." (Pierini,1999: p.17)

Como se ha podido observar el Hábeas Data es una garantía constitucional, cuyo objetivo es el de salvaguardar ciertos derechos inherentes a las personas, a través, del establecimiento de procedimientos que facilitan un libre acceso, actualización, modificación y supresión de los datos personales, que se encuentren contenidos en registros o bases de datos, sean éstas públicas o privadas.

IV.1.A DERECHOS PROTEGIDOS POR EL HÁBEAS DATA

El Hábeas Data como garantía constitucional establecida en nuestro ordenamiento jurídico está destinada a la protección de los siguientes derechos: derecho a la intimidad, derecho a la privacidad, derecho a la información y derecho a la autodeterminación informativa.

a) DERECHO A LA INTIMIDAD: Como se señaló en capítulos anteriores, el derecho a la intimidad es un derecho personalísimo, razón por la que es de posesión exclusiva y excluyente de los individuos. Este derecho hace alusión a ciertas manifestaciones de la persona como son la vida privada, familiar, el secreto, la inviolabilidad de domicilio y correspondencia, el honor, entre otros. Por tanto,

el papel que cumple el Hábeas Data es el de proporcionar una protección adecuada a toda aquella información relativa a la intimidad de las personas, incluyendo los aspectos que este derecho engloba, con el fin de evitar que información de carácter personal sea filtrada a terceros, que no posean interés legítimo. Así, Gozaíni manifiesta que el: *"Hábeas Data, a partir de la tutela de la intimidad, supone privilegiar la libertad de las personas para resolver qué aspectos de su vida permite que se hagan públicos a través de la información compilada o la difusión consecuente."* (Gozaíni,2001: p.74)

b) DERECHO A LA PRIVACIDAD: *"Privacy tiene un sentido activo que tiende a concretar la protección de los particulares impidiendo que terceros se ocupen de la vida privada de otros (...)"* En función con el Hábeas Data la protección de este derecho se da en dos sentidos: *"uno se dirige como mensaje impeditivo o barrera que se pone para evitar que la vida personal sea accesible a otros cuando el titular no lo admite; el restante, como acción positiva tendiente a obrar preventivamente frente a las agresiones provenientes de la informática."* (Gozaíni,2001: p.84,85)

c) DERECHO A LA INFORMACIÓN: Los bancos de datos almacenan una cantidad considerable de información de carácter personal, de ahí que, el hábeas data al garantizar el derecho a la información, se orienta a permitir el acceso a archivos, dentro de la fijación de ciertos límites. Así, se facilita la

actualización y corrección de los datos contenidos, dando lugar a una información veraz.

d) DERECHO A LA AUTODETERMINACIÓN INFORMATIVA: el cual se caracteriza por ser: *"a) Un derecho individual, previsto para atacar las intromisiones en la intimidad concretadas con un fin específico; b) Un derecho de acceso irrestricto, a excepción de fuentes de información que puedan mantener su secreto por razones de seguridad justificadas; c) Un derecho de requerir la verdad del registro, o de promover su rectificación o supresión; d) Un derecho de exigencia por el cual se pretende que el titular de la base de datos utilice la información compilada con la finalidad concreta para la que fue autorizado el archivo."* (Gozaíni,2001: p.107,108)

IV.1.B EL HÁBEAS DATA EN EL ECUADOR

En el año de 1994, durante el gobierno de Sixto Durán Ballén, se conformó una comisión conformada por 15 miembros, quienes tenían como fin el desarrollo de un anteproyecto, que introdujera posibles reformas constitucionales.

Hernán Salgado Pesantes indica que dentro de las propuestas realizadas para reformar la Constitución Política del Ecuador se encontraban, principalmente, una tendiente a sistematizar y actualizar los derechos fundamentales; y otra que estaba enfocada a definir las garantías de estos derechos. Dentro de la segunda se establecía como garantía la incorporación del hábeas

data. Estas reformas entraron en vigencia en el año de 1998.

La comisión al tratar el tema del hábeas data analizó el antecedente estipulado en el art. 32 de la Ley de Modernización del Estado, el cual trata sobre el acceso a documentos, estipulando que: *"Salvo lo dispuesto en leyes especiales, a fin de asegurar la mayor corrección de la actividad administrativa y promover su actuación imparcial, se reconoce a cualquiera que tenga interés en la tutela de situaciones jurídicamente protegidas, el derecho a acceso a documentos administrativos en poder del Estado y demás entes del sector público."*

Tomando en cuenta estas consideraciones, se procedió a redactar la norma constitucional que definirá al Hábeas Data. Teniendo como fin el dar a esta acción un sentido protector de los derechos de los titulares de los datos a ser informados sobre sí mismos, sobre sus bienes, y a conocer el uso y destino que tendrá la información recopilada, ya sea por entidades públicas o privadas. Además, se estableció el derecho del interesado de solicitar la actualización, rectificación, eliminación o anulación.

IV.1.B.a ESTRUCTURA DE LA NORMA CONSTITUCIONAL Y NORMAS REGLAMENTARIAS

NORMAS EXISTENTES

CONSTITUCIÓN POLÍTICA DEL ECUADOR

Art. 94 *"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en las entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional"*

LEY DE MODERNIZACIÓN DEL ESTADO

Art. 32 "Salvo lo dispuesto en leyes especiales, a fin de asegurar la mayor corrección de la actividad administrativa y promover su actuación imparcial, se reconoce a cualquiera que tenga interés en la tutela de situaciones jurídicamente protegidas, el derecho a acceso a documentos administrativos en poder del Estado y demás entes del sector público."

LEY DE CONTROL CONSTITUCIONAL, CAPÍTULO II: "DEL HABEAS DATA"

Art. 34 " Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya

dado o se les esté por dar, podrán interponer el recurso de Hábeas Data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de las personas que posean tales datos o informaciones."

Art. 35 "El hábeas data tendrá por objeto:

a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica.

b) Obtener el acceso directo a la información.

c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y,

d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado o no la ha divulgado."

Art. 36 "No es aplicable el Hábeas Data cuando afecte el sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan carácter de reservados por razones de Seguridad Nacional. No podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la ley deben mantenerse en archivo o registro públicos o privados."

Art.37 "La acción de Hábeas Data deberá interponerse ante cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos

requeridos. Los jueces o magistrado, avocarán conocimiento de inmediato, sin que exista causa alguna que justifique su inhibición, salvo cuando entre estos y el peticionario existan incompatibilidades de parentesco u otros señalados en la Ley."

Art. 38 "El juez o tribunal en el día hábil siguiente al de la presentación de la demanda convocará a las partes a audiencia, que se realizará dentro del plazo, de ocho días, diligencia de la cual se dejará constancia escrita. La respectiva resolución deberá dictarse en el término máximo de dos días, contados desde la fecha en que tuvo lugar la audiencia, aún si el demandado no asistiere a ella."

Art. 39 "Declarando con lugar el recurso, las entidades o personas requeridas entregarán, dentro del plazo de ocho días, toda la información y, bajo juramento, una explicación detallada que incluya por lo menos lo siguiente:

a) Las razones y fundamentos legales que amparen la información recopilada;

b) La fecha desde la cual tienen esa información;

c) El uso dado y el que se pretenderá dar a ella;
d) Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha de suministro y las razones para hacerlo;

e) El tipo de tecnología que se utiliza para almacenar a información; y,

f) Las medidas de seguridad aplicadas para precautelar dicha información.

Art. 40 "De considerarse insuficiente la respuesta, podrá solicitarse al juez que disponga la verificación directa, para la cual, se facilitará el acceso del interesado a las fuentes de información, proveyéndose el asesoramiento de peritos si así se solicitare."

Art.41 "Si de la información obtenida el interesado considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros, pedirá al juez que ordene al poseedor de la información que así proceda. El juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante. El depositario de la información dará estricto cumplimiento a lo ordenado por el juez, lo cual certificará bajo juramento, sin perjuicio de que ello se verifique por parte del propio interesado, solo o acompañado de peritos, previa autorización del juez del trámite. La resolución que deniegue el hábeas data será susceptible de apelación ante el Tribunal Constitucional, en el término de ocho días a partir de la notificación de la misma."

Art. 42 "Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por jueces o tribunales que concedan el Hábeas Data, no podrán ejercer ni directa, ni indirectamente, las actividades que venían desarrollando y que dieron lugar al Hábeas

Data, por el lapso de un año. Esta disposición será comunicada a los órganos de control y demás entidades públicas y privadas que sean del caso"

Art. 43 "Los funcionarios públicos de libre remoción que se nieguen a cumplir con las resoluciones que expidan los jueces o tribunales dentro del procedimiento del Hábeas Data serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se trate de funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por éste, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político. La sanción de destitución se comunicará inmediatamente a la Contraloría General del Estado y a la autoridad nominadora correspondiente."

Art. 44 " Las sanciones antes señaladas se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar."
Art. 45 Están legitimados para iniciar y continuar los procedimientos previstos en esta sección, no solo las personas naturales o jurídicas que consideren tener derecho a ello, sino también los padres, tutores y curadores en nombre de sus representados."

NATURALEZA JURÍDICA, OBJETO, BIENES JURÍDICOS PROTEGIDOS, POR EL HÁBEAS DATA, EN LA LEGISLACIÓN ECUATORIANA.

a) NATURALEZA JURÍDICA: La Constitución Política del Ecuador no estipula de forma expresa la naturaleza

del Hábeas Data, no obstante lo recoge dentro del capítulo de "Garantías de los Derechos", motivo por el que queda establecido que se trata de una garantía. Por otro lado, al revisar la normativa existente, se aprecia que la Ley de Control Constitucional contiene una confusión metodológica, puesto que se refiere al Hábeas data como un recurso y como una acción. El término correcto para el Hábeas Data es el de acción, en razón de que los recursos se interponen cuando ya se ha iniciado un proceso, y el recurrente se encuentra en disconformidad con la resolución vertida por la autoridad estatal. De lo que se deduce que el recurso se interpone, únicamente, ante decisiones de la autoridad estatal, mientras que el Hábeas Data puede ser dirigido contra personas naturales o personas jurídicas privadas.

b) OBJETO: El Hábeas Data constitucionalmente tiene como objeto:

a) El acceso a la información que sobre ella conste en un registro o en un banco de datos;

b) Conocer el destino de la información;

c) La actualización de los datos atrasados;
d) La rectificación de los datos inexactos;

e) La eliminación o anulación, en caso de que los datos erróneos o puedan afectar al titular de los mismos. Al revisar las normas legales se

encuentra que el objeto de la acción del Hábeas Data se amplía, de la siguiente manera:

a) Obtener del poseedor de la información que este la proporcione al recurrente, en forma completa, clara y verídica.

b) Obtener el acceso directo a la información.

c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y,

d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado o no la ha divulgado.

Por tal motivo, Puccinelli establece que en el Ecuador se encuentran los siguientes tipos de hábeas data: *"Al tenor de las facultades conferidas en el texto constitucional, se encuentran presentes en él los siguientes tipos de hábeas data: informativo, aditivo, rectificador o correctivo y exclusorio o cancelatorio. En la regulación subconstitucional, se pueden determinar los siguientes tipos: informativo, aditivo, reservador, rectificador o correctivo y exclutorio o cancelatorio."*(Puccinelli, 1999: p. 545)

c) BIENES JURÍDICOS PROTEGIDOS: Al respecto Puccinelli opina que:

a) En la formulación constitucional, el hábeas data está diseñado como un instituto suficientemente

amplio en el aspecto que s está analizando, esto es, con aptitud protectiva de la más variada gama de bienes jurídicos;

b) Sin embargo, por vía subconstitucional se ha recortado de alguna manera esta amplitud tutelar, toda vez que en la ley del control constitucional solo se autoriza la eliminación, rectificación o reserva en los casos de afección evidente de los derechos al honor, la buena reputación, la intimidad o en aquellos que se irrogue daño moral al solicitante;

c) Contrasta con esta limitación lo dispuesto por la ley de modernización del Estado que prevé el derecho de acceso con los amplios fines de asegurar la mayor corrección de la actividad administrativa y promover su actuación imparcial, y la tutela de situaciones jurídicamente protegidas" (Puccinelli,1999: p. 546)

IV.2 ¿POR QUÉ EL HÁBEAS DATA ES UNA HERRAMIENTA INSUFICIENTE PARA PROPORCIONAR UNA ADECUADA PROTECCIÓN A LOS DATOS PERSONALES?

La acción del Hábeas Data nace como respuesta a los avances de la informática, la cual abre la posibilidad de almacenar en archivos o bases de datos electrónicas grandes cantidades de información. Es así, como los datos personales proporcionados por los individuos a entidades públicas o privadas, se convierten en información procesada electrónicamente.

Hecho que coloca a los titulares de los datos en una posición de inseguridad, por cuanto existe un desconocimiento sobre los mecanismos de procesamiento, la distribución y el destino de la información.

La Constitución Política del Ecuador, en el Capítulo VI, de las Garantías de los Derechos - Sección II del Hábeas Data Art. 94 preescribe: " Toda persona tendrá derecho a acceder a los documentos, Bancos de Datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito". Razón por la cual considero, que el Hábeas Data constituye una garantía social, dirigida a precautelar los derechos de los titulares de los datos, en lo referente al manejo de su información. De tal modo, que esta institución protege varios derechos intrínsecos de la persona, como se ha manifestado anteriormente.

El Hábeas Data en la legislación ecuatoriana es concebido como una garantía, cuyo objetivo se dirige a:

a) que una persona pueda acceder a la información que sobre ella conste en un registro o en un banco de datos, en forma completa, clara y verídica;

b)conocer el destino de la información;

c)que se actualicen los datos atrasados;

d) que se rectifiquen los inexactos;

e) que se eliminen o anulen, en caso de ser erróneos o de afectar al titular de los mismos;

f) Que el responsable de los archivos o bases de datos donde se encuentra la información no la divulgue a terceros; y,

g) obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado o no la ha divulgado.

De lo que se puede colegir, que si bien el Hábeas Data proporciona ciertas garantías y seguridades a los titulares de datos personales; la forma en que se encuentra normada no es lo suficientemente específica, lo que origina que no se dé lugar a una protección adecuada de esta información.

Puccinelli, refiriéndose al caso ecuatoriano, opina que: *"Si bien el hábeas data- tanto en su faz constitucional, como en la subconstitucional - presenta ciertas deficiencias de índole técnica, en el diseño previsto en la ley fundamental ecuatoriana se presenta lo suficientemente amplio y permeable para que, por vía de reglamentación, se tutelen adecuadamente los derechos de las personas afectadas por el tratamiento manual o automatizado de datos personales."* (Puccinelli,1999: p.549)

De igual manera, Sarra al referirse al caso argentino, el cual guarda características similares a la legislación ecuatoriana, manifiesta que: *"Este precepto constitucional ha incorporado el hábeas data a*

nuestro ordenamiento jurídico. Ello constituye un intento de otorgar protección al individuo frente a la vulneración de sus libertades y garantías fundamentales, como consecuencia de la utilización indebida de sus datos personales. En realidad, esta medida no es suficiente, pues se requiere su reglamentación por medio de una legislación específica, como sucede a escala internacional." (Sarra, 2001: p.219)

Palazzi, al respecto, considera que es necesario que los Estados cuenten con Leyes de Privacidad y de Protección de Datos Personales, las cuales según su criterio *"pueden tener lugar bajo dos formas: a) una ley de carácter procesal, regulando aspectos tales como legitimación, competencia, medidas cautelares, apelaciones y demás cuestiones procesales del hábeas data, o b) una ley de carácter sustantivo, que establece reglas de protección de datos."* (Palazzi,2002: p.57)

Un ejemplo interesante, que se puede poner en consideración para la elaboración de una legislación específica de protección de datos personales, es el español con la LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPDAT).

Esta Ley incorpora los las disposiciones establecidas en la Directiva 46/95/CE, de 24 de octubre, la cual trata sobre la protección de las personas físicas en el tratamiento de datos personales y a la libre circulación de estos datos. Esta nueva norma deroga a la LORTAD, mas no muestra cambios

significativos, puesto que la toma como base e incorpora los principios dados por la Directiva, ampliando de esta forma su objeto.

De esta manera, la LOPDAT tiene como objeto *"garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, en especial el derecho al honor y a la intimidad personal y familiar, respecto al tratamiento de los datos de carácter personal(...) Su ámbito de aplicación, en consecuencia, se refiere a los datos personales registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de su uso posterior, en los sectores público y privado."* (Ull Pont, 2000: p.112)

Para lograr una adecuada protección a los datos de carácter personal, la LOPDAT ha incluido definiciones esenciales para el manejo de este tema como son:

a) DATOS DE CARÁCTER PERSONAL: cualquier información concerniente a personas físicas identificadas o identificables.

b) FICHERO: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) TRATAMIENTO DE DATOS: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación conservación, elaboración, modificación, bloqueo y cancelación, así como cesiones de datos que resulten de

comunicaciones, consultas, interconexiones y transferencias.

d) RESPONSABLE DEL FICHERO O TRATAMIENTO: Persona física, jurídica de naturaleza privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

e) AFECTADO O INTERESADO: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) PROCEDIMIENTO DE DISOCIACIÓN: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) ENCARGADO DEL TRATAMIENTO: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) CONSENTIMIENTO DEL INTERESADO: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) CESIÓN O COMUNICACIÓN DE DATOS: Toda revelación de datos realizada a una persona distinta del interesado.

j) FUENTES ACCESIBLES AL PÚBLICO: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Por otro lado, la LOPDAT dedica el título I para la enunciación de los principios de la protección de datos; el Título II para determinar los derechos de los titulares de los datos, respecto del tratamiento de esta información; y el título VI a la Agencia de Protección de Datos y su estatuto.

Dentro de los principios de protección de datos personales que contiene esta ley se encuentran los siguientes: calidad de los datos, derecho de información de los interesados en la recogida de datos, consentimiento del afectado y sus excepciones, tratamiento de datos especialmente protegidos, seguridad de los datos, deber de secreto respecto de los datos, condiciones de comunicación o cesión de los datos y condiciones de acceso outsourcer.

Los derechos de los titulares de los datos que norma la LOPDAT son: el derecho de acceso, el derecho de rectificación, el derecho de cancelación, el derecho de oposición, el derecho de tutela de los derechos anteriores, el derecho de indemnización y el derecho de impugnación de valores.

CAPÍTULO

V

PRINCIPIOS JURÍDICOS

APLICABLES A LA

PROTECCIÓN DE DATOS

PERSONALES

PRINCIPIOS JURÍDICOS APLICABLES A LA PROTECCIÓN DE DATOS PERSONALES

El avance informático y su trascendencia global ha hecho que la posibilidad de controlar el acceso a la información se torne, prácticamente, imposible. Sin embargo, el control para la difusión de la información es un requerimiento social a nivel mundial, que día a día se hace más necesario.

En primera instancia, tenemos que considerar que la protección a los datos personales, específicamente, del dato sensible; debe estar enmarcada dentro del respeto de ciertos principios, que deben constituirse en el referente de toda legislación. Así encontramos:

a) PRINCIPIO DE LA LIMITACIÓN DE LA RECOLECCIÓN DE DATOS: Impone la obligación de que toda la recolección de datos sea realizada por medios lícitos y legales. Y cuando fuese procedente con conocimiento y consentimiento del interesado. Así, hay prohibiciones de recolectar datos personales sensibles como las ideas políticas, religiosas o morales, costumbres sexuales, raza, uso de estupefacientes, entre otros.

Varios países han incorporado este principio a sus legislaciones. La Ley Francesa en su art.15 señala *"Excepto los casos en que deben ser autorizados por ley, los procesos automatizados de informaciones nominativas operados por cuenta del Estado, de un establecimiento público, de una colectividad territorial, o de una persona moral de derecho*

privado a cargo de un servicio público, serán determinadas por una ley o por una acta reglamentaria adoptada, previo despacho, por la Comisión Nacional de Informática y Libertades"

El art. 4 de la Ley Orgánica de Regulación al Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), ahora reemplazada por la LOPDAT, de España disponía: *"....En su clasificación (de los datos) solo podían utilizarse criterios que no se presten a prácticas ilícitas."*

En Gran Bretaña la *Data Protectión Act* de 1984 dice *"La información contenida en la Data Personal deberá ser obtenida y procesada en forma justa y de acuerdo a la ley."*

b) PRINCIPIO DE LA BUENA FE: este principio no es determinado taxativamente en las legislaciones, sino que la calificación de la forma en que el dato fue tratado es dejada a la sana crítica.

c) PRINCIPIO DE LA CALIDAD DE LOS DATOS: El dato personal debe ser adecuado, pertinente, no excesivo, exacto, veraz y actualizado, ya que conjuntamente estos tres elementos protegen al individuo. Este principio es fundamental ya que garantiza al individuo de que el dato personal por antigüedad o por mala calidad resulte falso. La LOPDAT en su art.4.1 dispone *"Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en*

relación con el ámbito de aplicación y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido", además prevé la rectificación o anulación del dato incorrecto, ya sea a petición de parte o de oficio. La Ley Francesa en su art. 37 establece que: *"Un archivo normativo deberá ser completado o corregido de oficio cuando el organismo que lo opera adquiera conocimiento de la inexactitud o del carácter incompleto de una información nominativa contenida en él."* La Ley Suiza, art.5: *"Toda persona que le concierne puede requerir la rectificación de los datos inexactos"*.

Asimismo, el Convenio 108 en su art.5.d dispone que los datos personales serán exactos y actualizados.

d) PRINCIPIO DE ESPECIFICACIÓN DEL FIN: Los datos no podrán ser recolectados sin tener un fin precisado, lícito y conocido por el titular del dato. La *Data Protection Act* expone que *"dicha información personal deberá ser poseída solo por uno o por propósitos específicos y que estén dentro de la ley"*.

e) PRINCIPIO DE RESTRICCIÓN DEL USO: El dato únicamente puede ser utilizado para la finalidad para la que fue requerido. Así, la LOPDAT en su art. 4.2 estipula que: *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos."*

f) PRINCIPIO DE LA JUSTIFICACIÓN SOCIAL: El dato requerido debe ser necesario y lógico para la sociedad al momento de su recolección. Este principio constituye un filtro protector contra las recolecciones con fines no lícitos o con apariencia de lícitos, pero que esconden fines contrarios a los valores de la sociedad.

g) PRINCIPIO DE CONFIDENCIALIDAD: El secreto del Dato Personal es protegido cuando se limita la recolección, se exige su exactitud y actualidad, y se limita su uso a la buena fe y al fin especificado. Pero el carácter de secreto del dato personal es de su propia esencia. Y si bien los principios enunciados protegen la intimidad y el consentimiento del afectado o la disposición de la ley hacen caer el carácter de secreto, no por ello se debe alterar la confidencialidad. Así, lo prevén los siguientes ordenamientos: La Ley Suiza art.7 *"Los datos personales deben ser protegidos contra todo tratamiento no autorizado por otros organismos o técnicas"* La LOPDAT, en lo referente al deber de secreto, señala que el responsable del fichero y quienes intervengan en cualquier fase de su tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo.

h) PRINCIPIO DE GARANTÍA DE SEGURIDAD: Los responsables de los bancos de datos deben procurar que los datos no lleguen a personas no autorizadas. Son

responsables por la pérdida o difusión no autorizada del dato. Al respecto, algunos sistemas jurídicos contienen la siguiente normativa: Ley Suiza art. 7 inc.1° *"Los datos personales deben ser protegidos contra todo tratamiento no autorizado."* Ley Francesa art.29 *"Toda persona que disponga o efectúe tratamiento de informaciones nominativas se comprometerá por tal hecho, en relación con la persona a quien le concierna, a tomar todas las precauciones necesarias para preservar la seguridad de las informaciones y especialmente para impedir que sean deformadas, truncadas o comunicadas a terceras personas."*

i) PRINCIPIO DE LA LIMITACIÓN EN EL TIEMPO: Cada dato es recolectado con un fin determinado, por ende no puede ser conservado más allá del tiempo necesario para ese fin, pues de lo contrario se atentaría contra el derecho a la intimidad. Al respecto la Ley Inglesa determina: *"La información personal que se posea para cualquier propósito o propósitos no deberá ser conservada por más tiempo del necesario para cumplir dicho propósito o propósitos."* Con relación a la obligación de conservar los datos personales durante el tiempo legal o destruirlos cuando el plazo haya vencido, la LOPDAT en el art. 16 numeral 5 estipula que: *"los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado."*

j) PRINCIPIO DE TRANSPARENCIA: La transparencia debe reflejarse en el manejo de los datos y en el desenvolvimiento de los bancos de datos. Así, se debe acceder con facilidad al conocimiento de la existencia de bancos de datos, de información sobre sus responsables y sobre el lugar donde ejercen la actividad.

k) PRINCIPIO DE LA PARTICIPACIÓN DEL INDIVIDUO: El titular del dato debe tener conciencia de sus derechos y hacerlos valer. Por otro lado, los responsables de los bancos de datos deben respetar ese derecho y no entorpecer su ejercicio.

l) PRINCIPIO DEL CONSENTIMIENTO DEL AFECTADO: En este ámbito hay que identificar tres posibilidades: 1. El afectado presta su consentimiento, en este caso se puede disponer del dato conforme al fin para el que se lo requirió y tomando las seguridades respectivas. 2. Cuando el interés público priva sobre el derecho a mantener en secreto algún dato personal y una ley así lo dispone. 3. Cuando los datos personales se recogen de fuentes accesibles al público; cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.

Al respecto la LOPDAT es muy clara, así, sostiene en el art.6 que:

1)El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2)No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3)El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4)En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.
(UCICH,1999:p.49-56)

LOPDAT.- Ley Orgánica de Protección de Datos de Carácter Personal de España.

CAPÍTULO

VI

NORMATIVIDAD

EXISTENTE

SOBRE PROTECCIÓN DE

DATOS PERSONALES

NORMATIVIDAD EXISTENTE SOBRE PROTECCIÓN DE DATOS PERSONALES

Al establecer los principios que rigen la protección de datos personales, hemos podido apreciar como ciertas legislaciones los han adoptado. En los países de América Latina, también, existe un interés por incorporar a sus ordenamientos jurídicos una legislación específica sobre la protección de datos personales, así algunos países ya han iniciado la elaboración de sus anteproyectos de ley. Por otro lado, cabe destacar que existe más normatividad acerca de este tema, la cual se procederá a determinarla.

a) La Constitución de Weimar de 1919, es la que marca el inicio del derecho a controlar los datos personales. Es así, como en su art. 129 se contemplaban estándares mínimos referentes al debido proceso, dando lugar al derecho de acceso al expediente.

b) En 1970, en Alemania, el Land de Hesse genera la primera ley dedicada, exclusivamente, a la problemática del tratamiento de datos personales.

c) Posteriormente, en el año de 1977 se sancionó la Ley Federal para la Protección contra el Uso Ilícito de Datos Personales, la cual se aplica a todo registro, ya sea automático o manual, público o privado, siempre que en éstos se procesen datos personales.

d) El Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: El avance de la telemática y las facilidades que ésta presta para el intercambio de información, ha hecho que se plantee la idea de que las legislaciones internas de los Estados son insuficientes en lo referente a la protección de datos personales. Así, algunos Estados han impuesto controles internos, en los que se requiere la autorización previa para exportar datos, esto sin embargo, implica una barrera para la libre circulación de la información; por tanto, era necesario llegar a un acuerdo internacional. Es así como surge el Convenio 108 de Europa, suscrito el 28 de enero de 1981, el cual *"pretende armonizar la necesidad de libre circulación de datos, con la protección de los derechos de la persona. (...) Se afirma que el objeto del Convenio es reforzar la protección de los datos, es decir, la protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal que les conciernen. Esto se ha hecho necesario por la creciente utilización de la informática para fines administrativos y de gestión."* (Ull Pont, 2000: p.54)

e) El Convenio de SCHENGEN, del 14 de julio de 1985: Este Convenio tiene por objetivo mantener ciertas libertades en sus relaciones con los países miembros. Se pretendía una libertad de circulación interior de mercancías, de servicios,

de capitales y de personas. Este espacio sin fronteras, para todas las personas que circulen en los territorios de los Estados participantes del acuerdo, trae consigo problemas de seguridad, por lo que es necesario establecer controles compartidos. Para esto se crea una base de datos común y de ahí nace la necesidad de incorporar normas que traten sobre la protección de los datos personales. Así, los Estados miembros deben respetar ciertas condiciones con relación al tratamiento de datos automatizados, las cuales están contenidas en el art.118: *"a) Control en la entrada de las instalaciones; b)Control de los soportes de datos, para impedir que puedan ser leídos, copiados, modificados o retirados por persona no autorizada;*

f) *Control de introducción, para evitar que se introduzcan sin autorización en el fichero, o que puedan conocerse, modificarse o suprimirse;*

g) *Control de utilización, para impedir que puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos ;*

h) *Control de acceso, garantizando que un sistema de tratamiento automatizado de datos, las personas autorizadas solo puedan acceder a los datos que sean de su competencia;*

i) *Control de la transmisión, que permita la posibilidad de verificar y comprobar a qué autoridades pueden ser remitidos datos de*

carácter personal, a través de las instalaciones de transmisión de datos;

j) *Control de introducción, garantizando que pueda verificarse y comprobarse a posteriori qué datos de carácter personal se han introducido en el sistema de tratamiento automatizado de datos, en qué momento y por qué persona han sido introducidos;*

k) *Control de transporte, por el que se impida que al empezar la transmisión de datos o durante ella puedan ser leídos, copiados, modificados o suprimidos sin autorización."* (Ull Pont,2000: p.64-65)

1) La LOPDAT, Ley Orgánica de Protección de Datos de Carácter Personal. Nace con el fin de incorporar los principios establecidos en la directiva 46/95/Ce, de 24 de octubre. Deroga a la Ley Orgánica de Regulación al Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), más no presenta cambios relevantes, únicamente, amplía su objeto e incorpora principios innovadores. Como se ha podido apreciar esta ley recoge varios de los principios expuestos anteriormente. Tiene como objeto *"garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, en especial el derecho al honor y a la intimidad personal y familiar, respecto al tratamiento de los datos de carácter personal"*, teniendo como fundamento el hecho de que los avances tecnológicos y de almacenamiento de información han colocado al derecho de la

intimidad y privacidad en una situación de inseguridad, causada por una amenaza antes desconocida.

m) El Código Modelo para la Protección de la Información Personal (Estándar Nacional de Canadá): este Código ha sido desarrollado por la Asociación de estándares Canadienses. Tiene como objetivo el establecimiento de estándares, que a través de su incorporación a entidades, se puede probar que se han tomado las medidas de seguridad apropiadas para proteger la información. Esta norma concibe la protección de datos personales *"desde dos ángulos diferentes: a) por un lado, se regula la forma en que las instituciones deberían recolectar, utilizar, divulgar y proteger la información personal, y b) por otro lado, se establecen disposiciones respecto del derecho de los individuos a obtener acceso a la información que les concierne y, en su caso, a corregir los datos erróneos."* (Sarra, 2001: p. 213)

Por último, es trascendental observar como la jurisprudencia ha recogido la aplicación de esta legislación y de los principios constitucionales relevantes en estos casos. Para esto se procederá a citar una jurisprudencia, cuyo contenido muestra la postura de la administración de justicia con relación a este tema.

"Es cierto que el uso de la información almacenada, procesada o distribuida a través de cualquier medio físico o electrónico se encuentra

suficientemente tutelado por normas constitucionales, como el derecho a trabajar y ejercer el comercio, de propiedad intelectual, inviolabilidad de la correspondencia, entre otros. Pero también es cierto que el productor, gestor y distribuidor de información debe respetar el honor, la privacidad y el goce completo de los derechos. Así, deben impedirse las intromisiones perturbadoras y la inadecuada difusión de datos procesados mediante los modernos adelantos tecnológicos cuando se afecta a la esfera íntima, tanto familiar como personal, haciendo ilusorias las garantías constitucionales" (C1a Cont. Adm., Córdoba, marzo 19 de 1995, "Flores, M.A. c/ Provincia de Córdoba", LLC,1996-316)

"El Tribunal Constitucional español en Sentencia dictada el 20 de junio de 1993 sobre el derecho al honor e intimidad, sobre la protección por el uso de la informática y sobre los ficheros con datos personales. Sienta jurisprudencia sobre el derecho a ser informado sobre ficheros automatizados de datos personales, vulnerando este derecho incluso el silencio administrativo, como respuesta a la solicitud del interesado. Se apoya jurídicamente en los arts. 10.2 y 18.4 de la Constitución, y en el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, sobre protección de la persona en el tratamiento de datos de carácter personal. Y esto aún cuando no hubiese sido promulgada la LORTAD 5/1992. Lo mismo cabe invocando la nueva Ley O., 15/1999, de Protección de Datos de Carácter Personal, que ha sustituido la LORTAD."

En estos fallos se demuestra el criterio de los tribunales, el cual se orienta a la defensa y

protección de los datos personales. Es fundamental considerar cómo la sentencia del Tribunal español es dictada tomando como fundamento, únicamente, los preceptos constitucionales. De esto se desprende, que en nuestro país se debe adquirir conciencia sobre la importancia de este tema, con el fin de que los administrados acudan a los órganos de justicia, para que, amparados en las normas constitucionales y legales existentes, hagan respetar sus derechos. De igual manera, esto constituiría un buen comienzo para impulsar la creación de una norma específica que regule la protección de datos personales, con el objetivo de proporcionar una mayor seguridad a los individuos.

CAPÍTULO

VII

CONCLUSIONES

Y

RECOMENDACIONES

CONCLUSIONES

En conclusión se puede apreciar que:

1. La sociedad de la información y comunicación, en la que hoy en día nos encontramos, ha traído cambios de magnitud dentro de los esquemas cotidianos del desarrollo de las actividades humanas. Dando lugar a nuevos conceptos e ideas en lo referente a técnicas y mecanismos de comunicación, información, administración, e incluso dentro de los hábitos y comportamientos del individuo.

2. Los avances de la tecnología proporcionan herramientas valiosas para hacer que las actividades diarias se desenvuelvan de una forma más eficaz y eficiente. Pero sobre todo este desarrollo tecnológico ha interpuesto nuevos retos, como individuos y como sociedad.

3. Una de las áreas más afectadas por el crecimiento tecnológico es el Derecho. Debido a que estos nuevos instrumentos, han dado lugar a nuevas formas de interrelación entre los individuos que forman parte de la comunidad.

4. Uno de los mayores avances tecnológicos es el relacionado con la informática. En virtud de que ésta permite y facilita el manejo de grandes

volúmenes de información, a través, de la utilización de medios electrónicos. De tal manera, se da origen a las nombradas bases de datos automatizados, las mismas que contienen información de todo tipo, entre la que se encuentran los datos personales de los individuos.

5. En el estudio antes realizado, se pudo observar cómo los datos personales poseen información que permite identificar a la persona.

6. Una deficiente protección de esta información podría dar lugar a la transgresión del derecho a la intimidad. Derecho que en nuestro ordenamiento posee un rango constitucional, por el hecho de ser una característica intrínseca del individuo. Así, la persona posee la facultad de conservar información dentro de su esfera individual, por considerar que estos datos no deben estar a disposición de terceros sin autorización.

7. El tratamiento de datos personales abarca lo referente a las distintas etapas del procesamiento de datos, como son la recopilación, grabación, conservación, organización, almacenamiento, modificación, actualización, relación evaluación, bloqueo, destrucción, cancelación y distribución de este tipo de información.

8. La preocupación por la protección de datos personales no es un tema que ha tomado importancia en este último período, sino que fue advertida en 1919 con la Constitución de Weimar, adquiriendo un mayor impulso en 1970. Desde entonces, tanto legislaciones como juristas han tratado lo referente a la vulneración de derechos, garantías y libertades de los individuos, como resultado de la recolección de datos en medios electrónicos.

9. La protección de datos personales constituye uno de los cimientos, en los que debe fundamentarse la normativa de la sociedad de la información. De ahí, que tratadistas de diferentes países como España, Estados Unidos, Suecia, Francia, Argentina, entre otros, han realizado valiosos estudios, que han permitido realizar legislaciones eficaces, dentro de sus países.

10. Dentro de la legislación ecuatoriana, se ha podido observar que tanto la norma constitucional como normas legales contienen reglas dirigidas a la protección de datos personales, como al establecimiento de mecanismos para alcanzar este propósito.

11. La Constitución Política del Ecuador establece la protección al derecho a la intimidad. Por otro lado, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su art. 9 enuncia que la protección de datos personales se

llevará a cabo tomando en cuenta los principios de intimidad, privacidad y confidencialidad. De igual manera, el Reglamento a la antes citada Ley, en su art. 21 define la obligación de las entidades públicas o privadas, a contar con mecanismos de seguridad para el manejo de datos personales, y la obligación de informar sobre éstos a los usuarios.

12. Con referencia a los mecanismos previstos para la protección de los datos personales, la Constitución en su art. 94 norma la institución del Hábeas Data. Acción mediante la cual se otorga al individuo el derecho de: *"acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en las entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización"*

13. La Ley de Control Constitucional, al normar al Hábeas Data, amplía los derechos de las personas, facultándolas para:

"a) Obtener del poseedor de la información que este la proporcione al recurrente, en forma completa, clara y verídica;

c) Obtener el acceso directo a la información;

c)Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y;

d)Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado o no la ha divulgado."

14. La acción del Hábeas Data, de acuerdo a la forma en que se encuentra contemplada dentro del ordenamiento jurídico ecuatoriano, no es una garantía suficiente para proteger los datos personales.

RECOMENDACIONES

1.- Como agentes activos de esta nueva sociedad se debe concienciar acerca de los cambios sustanciales que la introducción de las nuevas tecnologías han incorporado a la comunidad, y especialmente se tiene que visualizar los efectos que han ocasionado.

2.- Surje la inminente necesidad de regular estas nuevas formas de convivencia social, con el objetivo de que los derechos y garantías establecidos por los ordenamientos jurídicos, no se vean soslayados.

3.- Dentro de estos datos personales se encuentran los datos sensibles, los mismos que se refieren a las ideologías, creencias, religión, salud, orientación sexual y origen racial de los individuos. Información que por su naturaleza pertenece al fuero interno de las personas y que por tal motivo requiere de una protección especial, que impida que pueda ser obtenida y mal utilizada por terceros no autorizados.

4.- El tratamiento que se dé a los datos personales es esencial, para lograr una convivencia que respete los derechos de los seres humanos, dentro de esta sociedad tecnificada.

5.- Es necesario que los ordenamientos jurídicos establezcan estándares mínimos para el tratamiento, de tal forma, que los titulares de los datos tengan seguridad en lo referente al procesamiento de la información.

6.- Las entidades ya sean públicas o privadas, deben tener la obligación de informar a los usuarios sobre los mecanismos de procesamiento, y los derechos que los titulares de los datos poseen ante estas actividades.

7.- Al hacer un análisis sobre éstas y otras normas hemos podido concluir que la estructura jurídica que posee el Hábeas Data en nuestra legislación, si bien provee de los parámetros esenciales para la protección de datos personales, es evidente la necesidad de reglamentar al Hábeas Data con el fin de generar una adecuada protección.

8.- Se sugiere que se lleve a cabo la creación de una legislación específica que pueda abarcar todos los temas de concepto, principios y demás aspectos que se requieren para regular apropiadamente este tema. En este punto, es trascendental señalar que existe un desarrollo significativo en las legislaciones europeas, especialmente, en la Española, en donde vemos que si bien no existe una protección absoluta, se están instaurando los medios para alcanzarla.

9.- Es importante realizar un estudio sobre las mejores experiencias, con el fin de obtener referentes fundamentales para esta normativa. Asimismo, es importante poner en consideración los principios para la protección de datos personales, con el fin de que estos sean adoptados de la forma más coherente a nuestra legislación. De esta

manera, podremos realizar una legislación específica para la protección de datos personales, que tenga como base al Hábeas Data, pero que a la vez incorpore nuevas ideas, conceptos, derechos y tendencias, que satisfagan nuestra realidad, y que funcionen eficiente y eficazmente en nuestra sociedad.

10.- El derecho a la intimidad es propio de la naturaleza del individuo, por lo mismo, es trascendental brindar la protección adecuada a este derecho, contemplando todos los ámbitos de interferencia.

11.- La protección de datos personales en una era tecnológica es básica para el desarrollo íntegro del ser humano. Puesto que si no se toman medidas a tiempo, seremos cómplices de la información quebrantada con elementos esenciales de la persona como son su privacidad. De ahí, que se debe velar por el bien jurídico superior, que en este caso es el Derecho a la Intimidad.

BIBLIOGRAFÍA

DOCTRINA:

- Bibiana, Luz Clara, Manual de Derecho Informático, Editorial Nova Tesis, Buenos Aires, 2001.

- Cesario, Hábeas Data, Editorial Universidad, Buenos Aires, 2001.

- Ekmekdjian, Miguel Ángel, Hábeas Data el Derecho a la Intimidad frente a la Revolución Informática, Editorial Depalma, Buenos Aires, 1998.

- Fernández, Horacio, Internet: Su Problemática Jurídica, Editorial Abeledo-Perrot, Buenos Aires, 2001.

- Gozaíni, Osvaldo Alfredo, Hábeas Data Protección de Datos Personales, Editorial Rubinzal-Culzoni, Buenos Aires, 2001.

- Hernández, Giovanni, La Informática Jurídica, Ediciones Doctrina y Ley Ltda., Bogotá, 2000.

- Herrán Ortiz, Ana Isabel, La Violación de la Intimidad en la Protección de Datos Personales, Dykinson, Madrid, 1999.

- Lorenzetti, Ricardo, Comercio Electrónico, Editorial Abeledo-Perrrot, Buenos Aires, 2001.
- Palazzi, Pablo, La Transmisión Internacional y la Protección de la Privacidad, Editorial Ad-Hoc, Buenos Aires, 2002.
- Pérez Luño, Antonio Enrique, Del Hábeas Corpus al Hábeas Data, Editorial Aranzadi, Madrid, 1991.
- Pierini/Lorences/Tornabene, Hábeas Data Derecho a la Intimidad, Editorial Universidad, Buenos Aires, 1999.
- Puccinelli, Oscar, El Hábeas Data en Indoamérica, Editorial Temis, Bogotá, 1999.
- Sarra, Andrea Viviana, Comercio Electrónico y Derecho, Editorial Astrea, Buenos Aires 2001.
- Téllez Valdes, Julio, Derecho Informático, Editorial Mc. Graw Hill, México, 1998.
- Uicich, Rodolfo Daniel, Los Bancos de Datos y el Derecho a la Intimidad, Editorial AD-HOC, Buenos Aires, 1999.
- Ull Pont, Eugenio, Derecho Público de la Informática (Protección de Datos de Carácter Personal), Ediciones UNED, Madrid, 2000.
- Vázquez Gallo/ Berrocal Colmenarejo, Enrique/Julio, Comercio Electrónico Materiales para el Análisis,

ministerio de Fomento/ Ministerio de Ciencia y Tecnología, Madrid, 2000.

LEGISLACIÓN:

- Declaración Universal de los Derechos Humanos.
- Legislaciones internacionales: Francia, Suiza, Holanda, España, Argentina, Perú, Venezuela.
- LOPDAT, Ley Orgánica de Protección de Datos de Carácter Personal de España.

CONVENIOS Y TRATADOS INTERNACIONALES:

- El Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- El Convenio de SCHENGEN, del 14 de julio de 1985.

OTRAS HERRAMIENTAS:

- INTERNET
- Jurisprudencia
- *"No Hiding Place the protection of privacy will be a huge problem for the internet society"*, The Economist, 25 de enero de 2003.

LA PROTECCION DE DATOS PERSONALES EN LA LEGISLACION ECUATORIANA.

INDICE GENERAL

LA PROTECCION DE DATOS PERSONALES
EN LA LEGISLACION ECUATORIANA.

Por: Doctor: Carlos Espinosa Segovia

Tesis de Grado de Maestría aprobado en nombre del Instituto de Altos estudios nacionales por el siguiente Tribunal, a los veinticinco días del mes de marzo del dos mil cinco, Mención Honorífica (y) (o) Publicación.

_____ _____

C.C. C.C.

_____

C.C.

AUTORIZACION DE PUBLICACION

Autorizo al Instituto de Altos Estudios Nacionales la publicación de esta Tesis, de su bibliografía y anexos, como artículo de revista o como Artículo para lectura seleccionada o fuente de investigación.

Quito, marzo del 2005

.....

FIRMA DEL CURSANTE

Dr. Carlos Espinosa Segovia