FACULTAD DE DERECHO Y CIENCIAS SOCIALES

LAS MEDIDAS DE SEGURIDAD DE LAS BASES DE DATOS PERSONALES EN RELACION CON EL DERECHO A LA PROTECCIÓN DE DATOS EN ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesora Guía

Dra. Elsa Jacqueline Guerrero Carrera

Autor

Daniel Alejandro Merino Fiallos

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Elsa Jacqueline Guerrero Carrera

Doctora en Jurisprudencia

C.I.: 2000027470

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mí autoría, que se han citado las fuentes correspondientes y que en su ejecución, se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____

Daniel Alejandro Merino Fiallos

C.I.: 172122961-3

AGRADECIMIENTOS

Mi profundo agradecimiento a Dios, por toda su bondad, amor, misericordia y ayuda hacia mi persona. De la misma manera a mi Madre por su amor interminable, por su ejemplo y por no perder la FE en mí. A la UDLA que me ha permitido prepararme para desenvolver esta noble profesión. De manera especial a la Dra. Jacqueline Guerrero por dirigir el presente trabajo con dedicación y esfuerzo.

DEDICATORIA

A Dios y mi Señor Jesucristo, a mi Madrecita y mis hermanos Andrea y Julio por su amor y apoyo, ya que han sido los gestores de este logro, y a mi sobrinito que viene en camino, por ser una bendición para todos nosotros.

RESUMEN

Partiendo del derecho a la intimidad y en el contexto de la sociedad de la información, se ha configurado el derecho a la protección de datos personales, que consiste en garantizar el derecho de las personas a tener el control de datos que permiten identificarlos, por ello también se conoce como autodeterminación informativa.

La caracterización del derecho a la protección de datos tiene como un pilar fundamental al principio de seguridad, que implica el control, resguardo y cuidado que se deben proporcionar a los datos personales al momento de su tratamiento, por lo que los responsables del manejo o manipulación de dicha información deben adoptar medidas técnicas y organizativas indispensables para avalar la seguridad de los datos personales en la bases de datos o ficheros y así evitar que estos datos puedan alterarse, perderse o que sean manipulados indebidamente por terceros.

En el régimen de protección de datos personales la seguridad en el tratamiento de la información de cada individuo es sumamente importante y requiere de un ordenamiento jurídico organizado, así como de una normativa legal eficiente y moderna.

La Constitución de la República consagra el derecho a la protección de datos personales como un derecho de libertad, y lo garantiza mediante la acción de habeas data; sin embargo Ecuador no cuenta con una normativa secundaria específica, por lo que, en tema de seguridad en el tratamiento de datos personales, existe dispersión e ineficacia.

ABSTRACT

Departing from the right to the intimacy and in the context of the information society, the right has been formed to the protection of personal data, which consists of guaranteeing the right of the people to have the control of information that allow to identify them, for it also it is known as an informative self-determination.

The characterization of the right to the information protection has like a fundamental prop at the beginning of safety, which implies the control, security and care that must be provided to the personal data at the moment of it treatment, and the persons in charge of the handling or manipulation of the above mentioned information must adopt necessary technical and organizational measurements to endorse the safety of the personal data in the databases or files and this way to prevent this information from being able to falter, get lost or from manipulating unduly for third.

In the personal data protection the safety in the treatment of the information of every individual is extremely important and it needs of an organized juridical arranging, as well as of an efficient and modern legal regulation.

The Constitution of the Republic dedicates the right to the personal data protection like a freedom right, and byline guarantees it by means of the legal action of habeas data; nevertheless Ecuador is not provided with a specific secondary regulation, in safety topic in the personal data treatment, dispersion and inefficiency exists.

INDICE

INTRODUCCION

En el presente trabajo se analiza los aspectos fundamentales relacionados a la protección de datos personales, y el ámbito de la seguridad en las bases de datos personales, con referencia a las medidas de seguridad que son necesarias para garantizar el derecho a la protección de datos, tanto en Ecuador como en otros países.

En Ecuador existen disposiciones y normas dentro del marco legal ecuatoriano que hacen alusión a la protección de datos, pero de forma segregada y dispersa. Por ello se torna necesario que Ecuador cuente con una ley de protección de datos, que establezca el régimen de seguridad que debe aplicarse en el tratamiento de datos personales, a fin de evitar una violación del derecho constitucional.

La metodología que se aplicó para el desarrollo del trabajo fue un análisis de la doctrina; un análisis exegético de la ley, es decir relacionado con lo que las normas y disposiciones ecuatorianas señalan en cuanto al régimen de protección de datos personales y medidas de seguridad aplicables; así también se incluyó la realidad española y mexicana, a fin de establecer las diferentes posturas que existen sobre las seguridades en el manejo de datos.

El ensayo se estructuró en dos partes con el objetivo de abarcar la información más importante y relevante para el desarrollo y entendimiento de su contenido. En la primera parte se trató sobre la caracterización del derecho a la protección de datos personales y en la segunda parte se abordó la seguridad de los datos personales.

En el país se requiere de una ley de protección de datos personales que aporte al correcto y unificado entendimiento del tema, tanto para los responsables de las bases de datos o ficheros como para los mismos usuarios, mucho más si en algunos casos no se cuenta con medidas de seguridad específicas y que se encuentran estipuladas de forma dispersa como es el caso concreto del marco legal ecuatoriano.

PARTE I

CARACTERIZACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

En esta primera parte se analiza de forma clara y concisa el régimen de protección de datos personales, partiendo por la definición de datos personales, su clasificación, los derechos y principios dentro de este régimen; el derecho constitucional a la protección de datos en Ecuador y el marco legal secundario.

En la sociedad actual el uso de datos personales se ha vuelto, cada vez más, importante y fundamental en toda actividad. El resguardo y cuidado de la información personal, el hacer respetar los derechos y la adecuada acción por parte de terceros, ha permitido junto al avance tecnológico el desarrollo de la sociedad misma. Sin embargo es evidente que:

> "En la actualidad vivir en un mundo de constantes mejoras tecnológicas constituye un sin fin de beneficios para el sujeto. Sin embargo la utilización de medios tecnológicos como la Informática (ciencia del tratamiento automático de la información) ha originado un conglomerado de problemas jurídicos (…)" (Carbajal, 2005, parr.1).

En palabras de Sánchez (1998) "La información se ha convertido así en un medio tecnológico, formalizado jurídicamente, de enorme relevancia para la realización de múltiples actividades e iniciativas públicas y privadas" (p.26). Esta aparición de los sistemas informáticos como mecanismo para el traspaso de información, revolucionó los procesos y el desempeño de las empresas y entidades. Según Téllez (2004) "las computadoras, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de datos referidos a las personas" (p.60). Por eso la tecnología ha conseguido que se creen sistemas de bases de datos, las cuales posibilitan

archivar y almacenar información, contribuyendo con el desarrollo cada vez más acelerado y constante de la sociedad de la información; es decir, como lo señala León (2001) “la informática no es solo un fenómeno tecnológico de carácter objetivo” (p.81). Por lo tanto contribuye de manera ágil al tratamiento de la información en las bases de datos. Y debido al traspaso, almacenamiento y manejo de los datos de carácter personal, el derecho a la protección de datos ha ido evolucionando paulatinamente.

La protección de datos busca promover una real cautela por parte de los responsables o terceros. Para Serrano (2003, p. 23), este derecho a la protección de datos personales no solo empieza y termina con la recolección y el trato de los mismos, sino que perdura durante todo el tiempo en los cuales son requeridos y utilizados. Es por ello indispensable contar con una exhaustiva e inminente protección a las personas y sus datos con la finalidad de comprender los aspectos fundamentales de este derecho en la manipulación de la información personal, tema principal de la investigación.

1.1 Los datos de carácter personal: generalidades

Los datos de una persona han sido un elemento fundamental dentro de la comunicación o transferencia de información. Para Uicich (1999, p.40), dato es una referencia, siempre y cuando al ser humano no se lo establezca como tal, ni como un simple conjunto de datos. Es así que no se puede valorar a una persona por una simple recopilación de datos; sino más bien considerarlo como un individuo al que se lo identifica con sus datos o información. Por ende constituyen una pieza elemental de la identidad de las personas.

Al tener en cuenta lo establecido, los datos personales son la razón de ser del derecho a proteger datos propios o adquiridos del ser humano, y se les considera como “cualquier información concerniente a una persona física identificada o identificable” (Pampillo y Munive, 2012, p.266). Desde luego toda información personal de cada individuo es distinta, pero debe ser protegida de igual manera sin hacer distinción ya que se trata de un derecho para toda persona.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su glosario de términos, señala que datos personales “son aquellos datos o información de carácter personal o íntimo” (Disposición Novena). Esto quiere decir que son datos inherentes a los individuos, por tal motivo cada uno debe respetar la información personal del otro.

En la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, establece que un dato personal es “toda información sobre una persona física identificada e identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social” (Art. 2, Lit. a). Por consiguiente, se puede concluir que dato es una representación de información que en su conjunto determina un hecho; y los datos personales son toda la información que se refiere a una persona para identificarla, por ejemplo: por medio de su nombre, fecha de nacimiento, nacionalidad, sexo, estado civil, profesión, sus creencias religiosas, costumbres, entre otras; con toda esta información se puede realizar muchísimas actividades que todos llevan a cabo diariamente como estudiar, trabajar, optar por cualquier servicio, comprar, vender; y en fin un sinnúmero de actividades.

1.1.1 Clases de datos personales

Al conceptualizar los datos personales es necesario hacer un análisis sobre algunas de las diferentes clases que existen, siendo la principal distinción aquella que se realiza entre datos públicos y privados, a partir del acceso que se puede tener a los mismos con o sin el consentimiento de su titular. Se puede entender que cada dato personal tiene una carga implícita de información detallada de cada individuo, orientada a ser protegida como una necesidad en concreto (Hassemer y Chirino, 1997, p.7). Esta información se encuentra contenida en los diferentes archivos de bases de datos ya sean públicos o privados.

En el suplemento del Registro Oficial 162, de 31 de marzo de 2010, se publicó la Ley del Sistema Nacional de Registro de Datos Públicos, con el afán de regular y crear el sistema de registro de datos públicos en entidades públicas o privadas que almacenen y administren dichos registros. No obstante en el artículo 6 se hace alusión a datos privados de carácter sensible que pudiesen tener un uso público. Lo que se debe determinar es, cuáles datos específicamente, deben ser considerados como netamente públicos para separarlos de los privados (Guerrero, 2011, p.5), sin embargo en la ley analizada no se establece claramente su definición legal. Por tal motivo resulta imprescindible que se esclarezca idóneamente la definición legal de ambas clases de datos dentro de la ley, para una efectiva interpretación y aplicación.

1.1.1.1 Datos Públicos

Como su nombre bien lo indica son de acceso público, es decir de conocimiento de terceros sin necesidad de que el titular brinde su consentimiento, es así que se los define como:

> "aquellos datos personales que son conocidos por un número cuantioso de personas sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato; ni por la calidad del dato pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites de respeto y de convivencia cívicos (…)" (Davara, 2008, p.p.53-54).

Sin embargo, los datos públicos, pese a ser considerados como tales en el momento de su recopilación y difusión, requieren de igual cuidado que los demás datos de la persona titular, al ser más susceptibles de manipulación por terceros. Por su naturaleza, según Altmark y Molina (1998, p.166), los datos públicos son los recopilados y existentes en los organismos del Estado, cualquiera que estos sean, con lo que pueden encontrarse almacenados en la administración pública nacional, como las entidades provinciales y municipales, empresas públicas, sociedades del Estado, etc. No obstante, se discute si los

datos públicos al estar almacenados en bases de datos públicas deban ser relacionados como tales y no por su esencia o definición legal.

Por otro lado, mediante Resolución 007-NG-DINARDAP-2014, la Dirección Nacional de Registro de Datos Públicos aprobó las normas que regulan la asequibilidad a los datos personales que constan en registros públicos y clasifica la información personal de la siguiente manera:

a) Información restringida: Es toda aquella información que no es de acceso público y cuyo conocimiento, por parte de terceros, está condicionado al cumplimiento de determinados requisitos.
b) Información asequible: Es aquella información sobre la que existe alguna disposición legal que permite a terceras personas tener acceso a ella (Art.3).

Según esta norma, toda la información personal de un individuo se la considera restringida, y es accesible solo por excepción. En el caso de Ecuador, en el anexo B de la Resolución 007-NG-DINARDAP-2014, publicada en el Registro Oficial Suplemento 326 del 4 de septiembre de 2014, se enlistan los datos que tienen las diferentes instituciones públicas, que se consideran de asequibles, por tratarse de datos públicos. Así pues, se dispone un precepto de los datos públicos de libre acceso, por lo tanto se torna de vital trascendencia en el tratamiento de la información de los usuarios.

1.1.1.2 Datos Privados

En relación a este tipo de datos se los puede catalogar como muy sensibles para las personas, que al contrario de los datos públicos, no pueden ser de conocimiento de terceros sin la aprobación o permiso del titular.

Los datos privados se plantean como:

> “aquellos datos personales que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos, o ponerlos en conocimiento de terceros, siendo la

> conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular" (Davara, 2008, p.54).

Los datos privados se entienden como información "cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas (…)" (Ley Estatutaria de Protección de Datos Personales 1581, Art. 5). A propósito, en las circunstancias y situaciones en las que el titular es obligado a entregar sus datos personales privados, es prudente recalcar que esa misma voluntad de entregarlos debe estar respaldada por la finalidad con la que las entidades o terceros requieren de ellos, es decir que cada dato referido va a ser utilizado para el fin específico asignado y para nada más (Carbajal, 2005, parr. 8). Es así que cada dato privado debe cumplir con una función específica al momento de ser recopilados.

Dicho esto, los datos personales privados requieren tratarse con el mayor cuidado, control y sigilio por parte de los responsables de las bases de datos. Y de esta manera precautelar y garantizar la protección de la información de cada individuo, valga la aclaración, sin dejar de proteger a los demás tipos de datos.

1.1.2 Bases de Datos

Los datos personales tienen importancia per sé; sin embargo, su almacenamiento en bases de datos es lo que motiva preocupación y obliga a su protección, como menciona Uicich (1999) "la utilización discrecional de la información pone en peligro los derechos y libertades" (p.16). Es por eso que la seguridad en tema de protección de datos personales está directamente relacionada con las bases de datos que almacenan información de personas y resulta imprescindible. Por ello se debe clarificar también lo que se entiende por base de datos o ficheros.

Las bases de datos o ficheros han evolucionado de lo físico a lo digital, pero siempre han tenido esa función de archivar información. Tal y como lo manifiesta Yánez (1999) "las bases de datos son conjuntos organizados de

datos convertidos en documentación o información, con utilidad en distintas aplicaciones, dependiendo de su tratamiento para responder o no a determinada consulta.” (p.176). Es por eso que son tan relevantes para el archivo de los datos ya que los reservan de manera óptima para su posterior tratamiento.

Así también en la Ley de Propiedad Intelectual se establece una definición de lo que es una base de datos, la cual se entiende como una “compilación de obras, hechos o datos en forma impresa, en una unidad de almacenamiento de ordenador o de cualquier otra forma” (Art. 7). Dicho sea de paso, cada base de datos alberga un sinnúmero de información de cualquier tipo incluyendo datos personales de los individuos, y deben estar siempre organizadas y estructuradas para cada tipo de dato, para su tratamiento y su finalidad.

Las bases de datos se conocen también como ficheros, especialmente en el ámbito europeo. Conforme a la Directiva 95/46/CE un fichero de datos personales es “todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”. (Art. 2, Lit. c). Es así que los ficheros de entidades públicas o privadas deben incorporar siempre directrices de seguridad que serán acatadas por los responsables de su manejo.

En general las bases de datos ayudan a almacenar y ordenar la información de las personas, con el fin de estructurar un buen tratamiento y procesamiento de la misma, y por supuesto siempre deben estar destinadas a resguardar adecuadamente dicha información.

1.2 El derecho a la protección de datos: un derecho fundamental en la sociedad de la información

La transmisión y recepción de datos alrededor del mundo, ha contribuido a un óptimo crecimiento de la llamada sociedad de la información. Gracias a la aparición de nuevas tecnologías surge como uno de los fenómenos más trascendentales al facilitar la creación, el tratamiento y distribución de la información.

Cada vez más se pone en evidencia el auge y constante crecimiento de la sociedad de la información y la rapidez con que el ser humano se comunica, Téllez (2004) se refiere a la información como “una noción abstracta, no obstante que posee una connotación vinculada a una de las más grandes libertades, la de opinión y expresión de informaciones e ideas por cualquier medio que sea” (p.58). Este concepto de información es primordial porque la comunicación ha fortalecido y permitido el desarrollo de la humanidad. Resumiendo a Peña (2007) el intercambio de información a través de las tecnologías de información y comunicación han posibilitado la expansión de las comunicaciones, del comercio, de las relaciones entre las entidades públicas y compañías con los usuarios, de las relaciones entre personas y Estado, y en general con terceros (p.277). En resumidas cuentas el uso de las tecnologías en la transmisión y protección de datos o información, ha permitido el progreso a nivel mundial de la sociedad de la información conjuntamente con la globalización estableciendo herramientas novedosas para fortalecer la recepción y emisión de todo dato.

1.2.1 Consideraciones previas

Para comprender lo que engloba la protección de datos en toda su magnitud es necesario e imprescindible hablar sobre el derecho a la intimidad como su fuente primigenia. Para determinar un concepto de intimidad es primordial describir que es algo innato al ser humano, así lo dice Conde (2005), “el poder concedido a la persona sobre el conjunto de actividades que forman su círculo íntimo, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado” (p.22). Si tenemos a la intimidad como una esfera muy propia del ser humano, ésta se constituye plenamente en un parámetro para la no violencia de su espacio personal y de información que en él existe.

De igual manera para Pampillo y Munive (2012, p.159), se deriva como algo muy importante el hacer una comparación y diferenciar lo que tiene que ver con la vida privada e íntima de las personas, siendo que la primera, hace énfasis al entorno reservado de cada individuo, como lo manifiesta (León 2001) “el

arbitrio del hombre en su vida privada es, ante todo, una independencia para desarrollar sin que nadie lo interfiera" (p.86), es decir que las demás personas o terceros quedan relegados. La segunda se instituye como la faceta más personal de la vida y del ámbito familiar, cuyo saber se encuentra exclusivamente limitado al propio entorno familiar de cada sujeto. Por tal motivo es prudencial que más que reglar lo concerniente a la parte privada de cada individuo, son ellos mismos los que deben escoger qué información sobre sus datos van a dar a conocer, entregar y almacenar.

Así, el propio derecho va de la mano con la denominada autodeterminación informativa, la cual consiste en la capacidad de disponer de las personas de su propia información o datos y saberlos controlar (Guerrero, 2011, p.7). En otras palabras, determinar a qué persona o entidad se va a entregar dicha información, la finalidad a la que va a ser destinada dicha información y de qué manera se la entrega.

La protección de datos personales ha sido considerada un derecho de libertad de los ciudadanos, conforme lo previsto en la Constitución ecuatoriana vigente desde 2008, que surge a partir de la aparición de un fenómeno informático, que es la organización y sistematización de los datos. Esto sucede ya que con el surgimiento de sistemas informáticos se permite almacenar toda la información en bases de datos y así instaurar la defensa y protección de los datos personales frente a probables perjuicios al individuo (Hassemer y Chirino, 1997, p. 21). La obtención de datos personales se la realiza con el uso de medios tecnológicos y se puede emplear para diferentes fines, por ejemplo, obtener bases de datos de personas que tengan problemas de salud para no admitirlos en un seguro médico; u obtener datos de personas que no han pagado sus arriendos en seis meses para negarles el crédito para una vivienda.

El derecho a la protección de datos personales nace del derecho a la intimidad, ya que un tercero se está enterando u obteniendo información que no le compete o que no debería enterarse, es decir, la esfera más próxima e interior de la persona (Herrán, 2003, p.p.11-12). Este derecho con el tiempo logra independencia y autonomía; mientras que la intimidad requiere que alguien la

transgreda. La protección de datos personales es un derecho que proviene del titular, esto ligado a la autodeterminación informativa en que se “garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales” (Martínez, 2007, p.48). Es decir la persona dueña de los datos, es la única que sabe cómo manejar su información personal, incluso con el afán de conocer para qué están siendo recopilados. Por lo tanto el individuo debe tener la seguridad de que serán almacenados o utilizados para un determinado fin. Por eso son tan importantes las medidas de seguridad, pues se busca garantizar información que se transmite y que sean resguardadas con diferentes niveles de protección, de tal manera que una persona ajena a estas bases de datos obtenga información del titular.

A todo esto, existen derechos según la normativa europea que debe tener cada individuo para la protección y defensa de sus datos, mecanismos que controlen y cuiden de aquella información personal que está siendo manejada y controlada por terceros. Son tres tipos de derechos tradicionales, y uno nuevo llamado de oposición en materia de protección de datos; los cuatros se conocen como derechos ARCO: acceso, rectificación, cancelación y oposición. Se basan en el acceso de la persona titular a sus datos, la rectificación y cancelación de los datos cuando presenten alguna anomalía o irregularidad, y oposición o abstención a entregar información personal y que esta sea tratada y procesada para diversos fines (Serrano, 2003, p.p.343-369). En consecuencia los derechos ARCO establecen parámetros de seguridad en base a los derechos de cada individuo sobre el acceso, la finalidad, el estado, y la utilidad de su información, por consiguiente lograr un buen manejo y cuidado por parte de los tenedores de datos para alcanzar una ejecución óptima del tratamiento.

1.2.2 Principios de la protección de datos personales

Volviendo al marco general sobre la protección de datos personales, existen principios que rigen este derecho, a partir de los cuales se han construido los marcos regulatorios del derecho a la protección de datos personales. Peña

(2007) los establece como “principios esenciales por los que debe regirse un tratamiento de datos personales” (p.287). Los principios más importantes son:

- **Principio de Calidad de los Datos**: hace alusión a que los datos deben ser adecuados e idóneos, para su respectivo tratamiento, y así permitan cumplir con el objetivo para el que fueron recopilados. En este principio se garantiza el cancelar los datos cuando estos sean innecesarios, así como el actualizar o rectificar cuando estén incompletos o no corresponda al titular o interesado (Santos, 2005, p.100). En síntesis, para que este principio se cumpla todos los datos deben ser los correctos en cuanto a su validez e índole.

- **Principio de Transparencia o Derecho de Información**: está relacionado con los deberes que deben cumplir los responsables o terceros encargados de la recolección de los datos, es decir realizar un tratamiento de los datos de forma transparente, apropiada, justa y precisa, se obtengan con o sin previo consentimiento del propio interesado (Fernández, 2005, p.p.311-312). En pocas palabras, los datos pueden ser obtenidos de diferentes maneras siempre que se lo realice con responsabilidad y sin afectar al interesado.

- **Principio del Consentimiento Informado**: el tratamiento de los datos personales debería partir de lo que el titular desee entregar, compartir o traspasar, es decir de su propia voluntad. Pero lamentablemente esto no es una realidad, ya que solo en casos puntuales y específicos el consentimiento del interesado se pone en manifiesto, como por ejemplo cuando se trata de datos sensibles. Por otro lado se exceptuará el consentimiento cuando los datos se recopilen para las actividades y requerimientos de la función o administración pública (Guerrero, 2006, p.p.257-258). Por lo tanto el consentimiento se muestra como un paradigma para los propios usuarios, si se lo analiza de esa manera, ya que no todos sus datos requieren de su consentimiento para ser recolectados y procesados.

- **Principio de Seguridad**: este principio, es muy importante, sobre todo para el resguardo, control y seguridad que deben tener los datos al momento de su tratamiento; constituye un pilar fundamental para el derecho de protección de datos de carácter personal. Cada uno de los responsables de los ficheros o encargados del tratamiento tienen la obligación de amparar a los datos personales y sus titulares con mecanismos de seguridad técnicos y que garanticen el cuidado y protección de la información (Guerrero, 2006, p.p.279-280). Es así que las medidas de seguridad se corresponderán con los niveles de seguridad que se requiera acorde al tipo de dato personal; así, la protección puede ser baja, media o alta, según la sensibilidad del dato que se deba proteger.

Los principios de la protección de datos personales son muy importantes ya que establecen una guía y fundamentos esenciales sobre los cuales se promueve el apropiado manejo y procesamiento de la información de cada individuo por parte de los responsables de los ficheros, así como también se convierten en un respaldo para los usuarios en el afán de precautelar la protección de sus datos.

1.3 La protección de datos personales en Ecuador

En Ecuador la protección de datos personales tiene un escaso desarrollo normativo, pese a que ha existido referencia al tema desde el año 2002. Actualmente hay una dispersión y ausencia de normativa específica para desarrollar el derecho a la protección de datos, acorde al reconocimiento constitucional consagrado desde el 2008.

1.3.1 Reconocimiento constitucional del derecho a la protección de datos personales

En el ámbito constitucional, el derecho a la protección de datos en el país se consagra por primera vez en la Constitución de la República que entró en

vigencia el 20 de octubre de 2008. Siendo una Constitución renovadora, incorporó nuevos derechos como el referente a la protección de datos.

En el artículo 66, numeral 19, de la Constitución de la República del Ecuador se lo reconoce como un derecho de libertad, en los siguientes términos:

> "….incluye el acceso y la decisión sobre información y datos de éste carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución, o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley" (Constitución 2008).

Basándose en lo que se estipula en la Constitución, el principal objetivo sobre el cual se debe proteger a los derechos de los ciudadanos, es el resguardar y tratar los datos personales en todo el proceso de recopilación y tratamiento. Es decir, tal como lo señalan Páez y Acurio (2010) se busca "proteger al individuo ante el manejo o manipulación, no autorizada de sus datos personales que se encuentran en medios o formas electrónicas" (p.137). Todo con el fin de regular cualquier acto o hecho que afecte a las personas.

Para proteger los derechos de los ciudadanos, por ejemplo, está la garantía o acción de Habeas Data, que para León (2001) "se refiere al derecho que tiene la persona respecto a los datos guardados o recopilados por terceros" (p.91), y que se configura como el reconocimiento constitucional del derecho a la protección de datos. Por lo tanto "es una herramienta constitucional con que cuenta el ciudadano para controlar el tratamiento de sus datos personales" (Universidad de los Andes, 2003, p.393). Así pues esta acción constitucional constituye un pilar primordial para el eficaz control y protección de los datos, que en consecuencia se deriva en la correcta protección de los derechos del individuo.

La acción de Habeas Data se introdujo en 1997 a través de la Ley de Control Constitucional, hoy Ley Orgánica de Garantías Jurisdiccionales; pero con la relevancia e importancia del derecho a la protección de datos incorporado en la

Constitución actual. Es así que la acción de Habeas Data conforme al tenor del artículo 92, permite que toda persona, por sus propios derechos o como representante legitimado para el efecto, pueda ejercer la garantía con los siguientes fines:

1. Conocer la existencia y acceder a los documentos, datos genéticos, bancos o archivo de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, tanto en soporte material (papel) o electrónico.
2. Conocer el uso que se haga de los datos e información referida en el numeral anterior, así como su finalidad, origen y destino, y tiempo de vigencia del archivo o banco de datos.
3. Solicitar al responsable el acceso al archivo sin costo.
4. Solicitar la actualización, rectificación, eliminación o anulación de los datos.
5. En el caso de datos sensibles, exigir la adopción de las medidas de seguridad necesarias.

En definitiva la acción de Habeas Data se muestra como el principal mecanismo de protección constitucional de los derechos de cada individuo en el tratamiento de datos personales, con pautas que buscan garantizar dicha protección y que ponen de manifiesto la tutela por parte del Estado en favor de los ciudadanos y su información personal.

1.3.2 Marco Legal

A la fecha, Ecuador no cuenta con una ley de protección de datos personales que desarrolle el derecho reconocido en la Constitución de la República. Sin embargo en el ordenamiento jurídico si existen normas jurídicas que contienen disposiciones relativas a la protección de datos; esto genera una dispersión normativa que dificulta muchas veces el entendimiento del derecho.

Entre las normas que contienen disposiciones sobre protección de datos se cuentan: la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional; la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes

de Datos; la Ley del Sistema Nacional de Registros de Datos Públicos, entre otras. Por eso es conveniente un análisis sucinto de las disposiciones más importantes.

1.3.2.1 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

En el suplemento del Registro Oficial 52, de 22 de octubre de 2009, se publicó la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional cuyo propósito es regular la jurisdicción constitucional, con la finalidad de garantizar jurisdiccionalmente los derechos reconocidos en la Constitución, en los instrumentos internacionales de derechos humanos y de la naturaleza; así como garantizar la eficacia y supremacía constitucional.

> “La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos (...)” (Ley Orgánica de Garantía Jurisdiccionales y Control Constitucional, 2009, art. 49).

Por ende, el Hábeas Data, acción o garantía estipulada en el artículo 49 de esta Ley, es el arma fundamental que tienen los usuarios ante posibles vulneraciones al derecho a la protección de sus datos personales. Así como también autoriza judicialmente a toda persona al acceso de su información que se encuentre en poder de personas naturales, entidades públicas o privadas.

1.3.2.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

En abril de 2002 entró en vigencia la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, cuyo objetivo es regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

El artículo 9 de esta Ley fue una de las primeras disposiciones que hacía referencia a la protección de datos. En virtud de esta disposición se incorporó al ordenamiento jurídico ecuatoriano el principio del consentimiento informado, por el cual el consentimiento del titular es lo principal para la transmisión y procesamiento de datos, sin perjuicio de que en algunos casos no se requiere tal autorización ya que se trata de datos que son recopilados de fuentes públicas o por la administración pública en el ejercicio de sus competencias (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos). Así, el consentimiento informado se pone de manifiesto cuando se trata de datos sensibles de los ciudadanos y que no son de dominio público.

En el artículo 21 del Reglamento a la ley *ut supra*, se establece el principio de seguridad en la prestación de servicios electrónicos y transferencia de datos sensibles o datos personales, en las que el responsable de obtener los datos del titular, tiene que informar al mismo sobre los mecanismos de seguridad y todo lo concerniente a los sistemas de resguardo de sus datos. Sin embargo esto no se cumple a cabalidad y queda un vacío al no especificar las medidas o métodos de seguridad a utilizarse para garantizar el derecho a la protección de los datos. Si bien es cierto el tenedor de los datos se encarga de comunicar al usuario sobre dichos mecanismos, es prudencial que se encuentren señalados expresamente en la ley.

1.3.2.3 Ley del Sistema Nacional de Registro de Datos Públicos

En el Registro Oficial 162, de 31 de marzo de 2010 se publicó la Ley del Sistema Nacional de Registro de Datos Públicos, en cumplimiento de una de las disposiciones transitorias de la Constitución de la República que se puso en vigencia en octubre de 2008.

La ley que pretende regular el sistema de registros y su acceso, tiene como objetivo dar seguridad jurídica en el manejo, traspaso y resguardo para los datos públicos, ya sea en entidades públicas o privadas que manejen esta clase de información. En el artículo 6 de la Ley se encuentra estipulado que pueden existir datos sensibles o privados que podrían tener un uso en el ámbito público, sin embargo en la norma se vincula o relaciona la naturaleza pública de las instituciones o entidades con la naturaleza de los datos (Guerrero, 2011, p.1). Una observación muy valiosa en cuanto a si se debe denominar a un dato por su naturaleza o por su propia definición legal.

Existe una problemática en el contenido general de esta ley, cuya finalidad es crear y regular el sistema de registros de datos públicos y su respectivo acceso, como también respaldar la organización, interconexión y sistematización de toda la información que conste en sus registros. Esta ley regenta para las entidades del sector público y privado que administren bases de datos públicos, sobre las personas naturales o jurídicas, sobre sus bienes o patrimonio. Esta inclusión de las entidades privadas, surgió a raíz de que, según la comisión legislativa que analizó el proyecto de Ley, existen entidades privadas que pudiesen tener a su cargo bases de datos públicas, como fundaciones, corporaciones, etc (Guerrero, 2011, p.4). Sin embargo hay que analizar que se entiende por sistema, registros y la terminología de “datos públicos”, ya que existen casos en que dichos datos son de naturaleza privada o sensible, o así deberían serlo pero son manejados por la relación que tienen con las bases de datos donde se encuentran almacenados, y cabe la duda de cuándo o por qué van a ser manejados estos datos de diferente manera.

En razón de la Ley, se creó la Dirección Nacional de Registro de Datos Públicos, DINARDAP, como una entidad dependiente del Ministerio de Telecomunicaciones y de la Sociedad de la Información. Desde su creación la DINARDAP ha emitido varias resoluciones que tienen relación con el tratamiento de datos personales, por lo que estas normas deben ser parte del análisis cuando se trata de protección de datos.

1.3.2.4 Ley Orgánica de Telecomunicaciones

La Ley Orgánica de Telecomunicaciones, publicada en el Registro Oficial 439, de 18 de febrero de 2015 contiene en su artículo 78, lo que representa dentro del ámbito de la protección de datos, el debido cuidado y vigencia del derecho a la intimidad que tienen los usuarios y que se encuentra establecido en el artículo 66 numeral 20, el cual señala el derecho a la intimidad personal y familiar de los individuos. En esta ley se menciona también que los prestadores de servicios de telecomunicaciones deberán garantizar la protección de los datos de carácter personal, con la adopción de medidas de seguridad como mecanismos necesarios e indispensables que efectivamente aseguren la protección de la información personal.

Por otra parte el artículo 79 establece, que en casos de violación de datos personales, el abonado o usuario, es decir el titular de los datos; puede recurrir a medidas de seguridad para mitigar el daño que se ha causado. Como punto muy importante cabe recalcar que se determina como violación a la falta de seguridad de los datos personales. Aquí se pretende efectivizar el resguardo y cuidado de la información de cada una de las personas que se benefician del servicio en telecomunicaciones, como por ejemplo cuando se contrata un plan, una promoción, etc.

1.3.2.5 Reglamento para Interoperabilidad de Información de Identificación

Mediante Resolución del Registro Civil No. 307, de 28 de junio de 2013, se promulgó el Reglamento para Prestación del Servicio de Consulta, Transferencia e Intercambio de la Información de Identificación, contenida en

los Registros de Datos Públicos de la Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC), el cual señala en su artículo 7 a los principios de seguridad y confidencialidad para el resguardo y sigilio de los datos personales confidenciales. También se establece la custodia de la información, es decir que la Dirección General de Registro Civil, Identificación y Cedulación constituye el único responsable de la protección y control de la información, registros y bases de datos que se encuentren a su cargo.

Estas normas, que conforman el sistema u ordenamiento jurídico ecuatoriano, muestran una parte del ámbito de la protección de datos que se maneja dentro del país en las diferentes áreas; estableciendo las principales disposiciones para el tratamiento y resguardo de cada uno de los datos personales de los usuarios, los mecanismos que se emplean para el efecto, y las falencias que existen en ellas.

PARTE II

LA SEGURIDAD DE LOS DATOS PERSONALES

En esta segunda parte se analiza el principio de seguridad, así como las medidas de seguridad en el manejo de datos personales, tanto desde la experiencia española como desde la experiencia mexicana; para esto se detalla los niveles de seguridad, algunos de los estándares internacionales y el Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Por último se realiza un análisis en concreto sobre la realidad ecuatoriana.

La seguridad que se debe tener en la manipulación de datos personales de los individuos es un tema de suma importancia, para garantizar el derecho a la protección de datos. La cautela y cuidado con que se maneje cada base de dato, el sigilio con que se realice el tratamiento de la información y la responsabilidad con que se procesen los datos, son parámetros indispensables para una adecuada seguridad de los datos.

Tal y como lo expresa Fernández:

> “El tratamiento automatizado de la información no está exento de riesgos y peligros, entre los que se muestra como preferente atender al respeto debido a las personas ante el derecho fundamental de nueva creación que se ha dado en denominar: derecho fundamental a la protección de datos” (2005, p.125).

Esto establece un precepto inalterable, en cuanto a que cada información almacenada y detallada en todas las bases de datos debe ser cuidadosamente tratada, cualquiera que fuese su tipo o naturaleza; la seguridad debe reflejarse en todo proceso. En las entidades privadas así como en las públicas, el manejo del sistema de registros de datos está enfocado en brindar servicios a sus usuarios, protegiendo sus respectivas bases de datos; por lo que se buscan alternativas que mejoren constantemente la calidad del servicio y la seguridad

de la información (Herrán, 2003, p.p. 35-37), todo esto con un fin determinado, el proteger al usuario y sus derechos. Como lo manifiestan Hassemer y Chirino (1997) “entre más grande es el peligro más nítidas deben ser las medidas a tomar” (p.16), algo muy razonable y cierto en el deber de protección a los datos personales en base al principio de seguridad, que busca defender los intereses de cada persona al utilizar mecanismos y estándares internacionales de protección.

2.1 Del principio de Seguridad

El principio de seguridad en la protección de datos es trascendente para el cuidado de cada uno de los datos, que se encuentran registrados en las bases de las diferentes entidades o instituciones públicas o privadas. Como afirma Uicich (1999) respecto a los encargados del tratamiento de datos personales “son responsables por la pérdida o difusión no autorizada del dato” (p.53). En el tratamiento de los datos personales existe un riesgo latente que pone en peligro el resguardo y buen manejo de los mismos, como cuando los datos son inexactos o incompletos, no se encuentren actualizados, no son los relativos a la persona, o también que puedan ser usados por motivos ilegales o fraudulentos. La seguridad de la información que se maneja en cada base de datos se establece como un elemento clave en la actualidad, esto debido a la forma tan acelerada que se transmite y procesa la información.

Así pues, Guibourg, Alende y Campanella (1996), señalan lo que contempla la seguridad de datos:

> “La información ha de hallarse adecuadamente protegida en los registros en los que se la almacene, de tal modo que no sea susceptible de destrucción, adulteración o acceso indebido por terceras personas. Esta necesidad requiere ciertas medidas técnicas y administrativas, así como una formación ético-profesional del personal encargado de administrar y manejar los registros” (p.p.265-266).

En consecuencia lo que los autores determinan, es una idea clara y concreta de lo que conlleva la seguridad de los datos, aun teniendo en cuenta que su noción tiene veinte años de ser expuesta. Es así porque resulta sustancial el proteger a la información, de la manipulación indebida y prohibida por parte de terceros, como también la responsabilidad y mecanismos con que los responsables de manipular los datos deben procesar la información.

Entonces, si bien es cierto que existen riesgos que pueden presentarse en el tratamiento de los datos personales por parte de los encargados o responsables de manejar cada base de datos o ficheros, también es cierto que estos riesgos pueden provenir del uso o manipulación de datos personales por parte de personas que no estén autorizadas a recopilar, acceder, o manipular los datos. Resumiendo a Sánchez (1998, p. 196), la oportuna seguridad que tengan los datos que son procesados y almacenados de forma electrónica, para contrarrestar cualquier riesgo o peligro inminente, ayuda a garantizar los derechos de las personas y la protección de sus datos personales. En consecuencia también resulta apropiado un avance y mejora en los mecanismos de protección tanto dentro del ámbito legal como del técnico.

Es así que este principio determina que cada dato personal debe tener un tratamiento óptimo, asegurando el buen procedimiento y uso que se dé a la información de cada persona y así se logre evidenciar la protección de sus derechos (Martínez, 2007, p.144). La seguridad implica avalar la confidencialidad, la integridad y la disponibilidad de los datos. Por tal motivo para Serrano (2003, p.p. 452-453), la confidencialidad se refiere a la potestad de conocer los datos únicamente por las personas que han sido autorizadas para aquello, por ende las demás personas no autorizadas, están privadas de esta potestad. La integridad hace referencia a que los datos no pueden ser alterados de manera indebida por los responsables de los ficheros, es decir representa una seguridad o garantía de que los datos, como su nombre lo indica, son íntegros, correctos, exactos y completos. Y por último la disponibilidad contempla el acceso permitido de los datos personales o información, a las personas autorizadas para aquello, cuando crean

conveniente y necesario. Pues bien, en su conjunto estos tres elementos estructuran un sistema de resguardo y control que busca cuidar los datos y no permitir la violación de la información, al establecer también un escudo contra el acceso no permitido o ilegal, como por ejemplo lo que realizan los hackers y delincuentes informáticos.

2.2 Medidas de Seguridad

Los mecanismos que se adopten para brindar una seguridad idónea en la protección de datos, dan lugar a un correcto y cuidadoso control de los mismos, es decir garantizan el principio de seguridad. Existen medidas de seguridad que permiten un tratamiento pertinente de la información, y que brindan la seguridad requerida para optimizar la calidad del procesamiento de datos.

En consecuencia, estos mecanismos son preponderantes en la búsqueda de prevenir riesgos y peligros para la información personal. Galindo expone su pensamiento sobre las medidas de seguridad:

> “Por lo general si se estudian propuestas que emanan del terreno informático se encuentra en ellas que, bajo la denominación de medidas de seguridad de los sistemas de información y comunicación, se incluyen especialmente aquellos mecanismos y prácticas profesionales que facilitan un uso continuado de las tecnologías, así como la prevención de acciones destinadas a interrumpir o sabotear su funcionamiento o la interpretación de datos elaborados y tratados por otros” (1998, p.67).

En relación con las medidas de seguridad en el tratamiento de datos personales el análisis se enriquece si se lo realiza a partir de experiencias concretas. Por esta razón se describe el tratamiento que España y México han dado al tema de la seguridad en los datos.

2.2.1 La experiencia española

El tratamiento que España ha dado al tema de la seguridad en la protección de datos está basado en los niveles de medidas de seguridad que serán aplicadas según el tipo de dato que se encuentra almacenado en bases de datos o ficheros, y se configura desde una perspectiva jurídica. Todo tipo de dato necesita ser manejado y tratado eficientemente, y ésta ponderación ayuda a que este proceso de seguridad y tratamiento sea más detallado, más minucioso (Conde, 2005, p.50). Aunque también resulta muchas veces extremadamente complicado, al momento de ponderar y determinar qué datos requieren de determinada seguridad y que datos no.

Estas medidas de seguridad se clasifican en nivel bajo o básico, medio y alto. Es así que por ejemplo se aplica un nivel bajo de seguridad si se trata de datos como el nombre o número de hijos de un individuo; nivel mediano o medio de seguridad para datos como el número de calzado o la cédula de identidad; y medidas de nivel alto para datos muy sensibles como la filiación política de un individuo o su historial crediticio.

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece que:

> “El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.”

Los países no tienen incorporadas en las normas, disposiciones sobre las medidas de seguridad que se deben tener para proteger los datos personales,

a excepción de la norma española. Por tanto aquella se considera un nuevo paradigma en tema de medidas de seguridad para protección de datos.

De acuerdo a Santos (2005, p.p. 140-141), “las medidas de seguridad deben implantarse en los ficheros automatizados de datos personales, los centros de tratamiento de datos personales, locales, equipos, sistemas y programas que alberguen o sometan a tratamiento datos personales”. Cada una de las medidas, en sus diferentes niveles otorga un control y cuidado necesario, debido a la susceptibilidad e importancia que posea cada tipo de dato. Los datos personales constituyen uno de los elementos más valiosos de las empresas y entidades, y por tal razón cada una de ellas debe contar con herramientas de seguridad que permitan una adecuada conservación y manejo de los datos personales.

De acuerdo al Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en relación con lo que determinan los artículos 79, 80 y 81, se muestra lo relacionado a las medidas de seguridad en el tratamiento de carácter personal, en la cual determina que las medidas o niveles de seguridad exigidos a los tratamientos y ficheros se clasifican en básico o bajo, medio y alto, como también señala que:

Las medidas de seguridad de nivel básico o bajo se contemplan:

- En general, los datos de carácter personal que contenga cualquier fichero.
- Los datos de carácter excepcional, datos sobre ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual cuando su finalidad sea la transferencia dineraria a entidades de las que los afectados sean asociados o miembros. Cuando sean datos objeto de un tratamiento accesorio o incidental que no se relacionen con la finalidad del fichero. Y en los ficheros en donde se encuentren datos de salud, referidos únicamente al grado o condición de discapacidad o invalidez, con motivo del cumplimiento de deberes públicos.

Las medidas de seguridad de nivel medio deben ser aplicadas por el responsable del fichero en el tratamiento cuando se trate de:

- Datos relativos a la comisión de infracciones administrativas o penales.
- Los relativos a la prestación de servicios de solvencia patrimonial y crédito.
- Datos de las administraciones tributarias, relacionados con el ejercicio de sus potestades.
- Datos de entidades financieras, para las finalidades de la prestación de servicios financieros.
- Datos de entidades gestoras y servicios comunes de seguridad social, en el ejercicio de sus competencias.
- Datos de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Los datos que permitan una definición de la personalidad o característica de un ciudadano, y que ayuden a evaluar los determinados aspectos de su comportamiento y personalidad.

Las medidas de seguridad altas tienen que ser aplicadas por el responsable del fichero en el tratamiento cuando se trate de:

- Datos que se refieran a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Datos derivados de actos de violencia de género (Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, 2007).

En referencia a lo señalado, el encargado o responsable del fichero que realice el tratamiento de datos que requieran un nivel medio de seguridad, deberá implementar también las medidas de nivel básico. Y en el caso que el fichero realice el tratamiento de datos que requieran un nivel alto de seguridad, tendrá que implementar conjuntamente las medidas de nivel medio y bajo. Para Galindo (1998), las medidas de seguridad tienen que ser concebidas como

prácticas apropiadas para lograr un proceder correcto en el manejo de los datos (p.68), y de hecho lo que contempla la legislación española es justamente que los responsables de los ficheros actúen adecuadamente en sus funciones.

En conclusión, en este tipo de enfoque los lineamientos que se aplican están basados en la protección y definición jurídica por el tipo de datos, no importa el sistema que ocupe, la finalidad es otorgar un nivel de protección alto, mediano o bajo a determinados datos. Tratándose del tema de seguridad en el tratamiento de los datos personales se considera que la normativa española es un referente adecuado para Ecuador, pues al no regular una tecnología específica, se asegura que la norma no quede obsoleta cuando la tecnología cambie.

2.2.2 La experiencia mexicana

En este enfoque se maneja una percepción sobre las medidas de seguridad desde la visión técnica, estableciendo para proteger a los datos personales, sistemas, modelos o medidas técnicas, por ejemplo el Sistema de Gestión de Seguridad de Datos Personales (SGSDP), que brinden una adecuada garantía en cuanto al cuidado y protección de la información personal.

En síntesis, es necesario e importante señalar que en diferentes entornos se encuentran desarrolladas otras herramientas y recursos en base al principio de seguridad para la protección de datos, recursos técnicos y procedimientos específicos como estándares internacionales y las llamadas normas ISO (Blanco, 2015, p.49). Es por eso que México se encuentra entre los entornos que han desarrollado recursos técnicos para la seguridad en la protección de datos personales y en el tratamiento controlado e informado.

El artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares señala que:

> “Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad,

> administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado".

Es decir estipula la obligación y el deber de las personas encargadas del manejo de datos personales a que contemplen en su accionar, las herramientas de seguridad que resguarden a los datos personales de los usuarios. Aquello busca garantizar la efectividad del derecho a la protección de datos personales.

2.2.2.1 Sistema de Gestión de Seguridad de Datos Personales

El INAI o Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México en su Documento Oficial *Recomendaciones en Materia de Seguridad de Datos Personales*, publicado el 30 de octubre de 2013, establece para la protección de datos la admisión de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), estructurado con las fases PHVA (planear, hacer, verificar, actuar).

El sistema de gestión de seguridad de datos personales se establece como un "procedimiento general para operar, monitorear, revisar, y mejorar el tratamiento y cuidado de los datos personales" (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 2013). Por lo tanto, este sistema de gestión tiene como finalidad proporcionar una estructura de operación en el tratamiento de datos personales para los responsables de los ficheros y así continuar mejorando las prácticas óptimas de seguridad de los datos personales y el adecuado cumplimiento de la ley.

Conforme lo establece el INAI en su documento oficial, el proceso del sistema de gestión de seguridad de datos personales, según las fases PHVA:

Como primer punto se encuentra el planificar o planear el SGSDP, es decir plantear los alcances y objetivos, la política de gestión de los datos personales, determinar las funciones y obligaciones de quienes realicen el tratamiento, así como también realizar un inventario de aquella información y un análisis de

riesgo de los datos personales para identificar las medidas de seguridad a plantearse dependiendo del caso. Luego viene la fase de hacer el SGSDP, es decir la implementación de las medidas de seguridad aplicables a cada dato personal. Después se debe verificar el SGSDP, en otras palabras, evaluar el funcionamiento del SGSDP según la política determinada y conforme a la ley. Por último actuar con el SGSDP, mejorando continuamente y capacitando al personal de acuerdo a los resultados obtenidos con este sistema de protección de datos personales. (Recomendaciones en Materia de Seguridad de Datos Personales, 2013). Teniendo en cuenta el proceso con el que se maneja el Sistema de Gestión de Seguridad de Datos Personales, la seguridad de los datos se plantea desde una perspectiva sistematizada y concreta de una serie de etapas en las que los datos son tratados.

2.2.2.2 Estándares internacionales

Los estándares internacionales o modelos que se plantean alrededor del mundo son primordiales para el ámbito de protección de datos personales, de acuerdo al propio INAI muchos de éstos constituyen fundamentales para las acciones y funcionamiento del proceso de seguridad en el tratamiento de los datos personales de los individuos, como lo son para el caso del Sistema de Gestión de Seguridad de Datos Personales. Entre algunos que el INAI hace mención en su Documento Oficial *Recomendaciones en Materia de Seguridad de Datos Personales*, están:

- BS 10012:2009, Data protection. Specification for a personal information management system.
- ISO/IEC 27001:2005, Information technology security techniques. Information security management systems requirements.
- ISO/IEC 27002:2005, Information technology security techniques code of practice for security management.
- ISO/IEC 27005:2008, Information technology security techniques information security risk management.
- ISO/IEC 29100:2011, Information technology security techniques privacy framework.

- ISO 31000:2009, Risk management principles and guidelines.
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards.
- ISO GUIDE 73, Risk management vocabulary.
- ISO 9000:2005, Quality management systems fundamentals and vocabulary.
- NIST SP 800-14, Generally accepted principles and practices for securing information technology systems.
- OECD Guidelines for the security of information systems and networks towards a culture of security.

Los temas de seguridad en el manejo de datos personales incluye también las políticas de privacidad, en las que se reflejan los mecanismos de seguridad que el responsable adopta y pone en conocimiento de los titulares de los datos. A nivel mundial la transmisión de datos personales es descomunal, a decir de Peña (2007) “el proceso automático y los flujos transfronterizos de datos personales crean nuevas formas de relación entre países y exigen la elaboración de normas y prácticas de seguridad” (p.279). España y México son dos referentes importantes en el ámbito de la protección de datos personales, ya que establecen mecanismos organizados y estructurados para garantizar el control y buen manejo de la información de las personas, España desde una apreciación jurídica y México desde una más técnica. Ambos han contribuido al desarrollo y fortalecimiento de la seguridad en el tratamiento de datos personales.

2.3 La realidad ecuatoriana

Sobre el tema de la seguridad en el manejo de datos personales se ha desarrollado y tratado mucho en el ámbito internacional, tal es el ejemplo de España y México, sin embargo, es un tema relativamente reciente en Ecuador. Tal y como se ha señalado, existe una dispersión normativa que puede llegar a perjudicar y dificultar la aplicación y entendimiento del derecho a la protección de datos, pues el país no cuenta con una ley de protección de datos.

2.3.1 Disposiciones legales

En general, para cualquier base de datos que contenga datos personales el artículo 92 de la Constitución, sería aplicable. Además de las medidas de acceso, rectificación y eliminación, esta garantía jurisdiccional también permite solicitar que el tenedor de datos personales adopte medidas de seguridad, por lo tanto se manifiesta como la primera disposición en el ordenamiento jurídico en relación al tema de la seguridad de las bases de datos personales. Desde luego existen otras disposiciones que enuncian el tema de la seguridad de los datos personales, las cuales se procederá a analizar.

El Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos contiene un artículo, el cual establece la obligatoriedad de adoptar sistemas seguros, pero es aplicable a los prestadores de servicios electrónicos, porque el ámbito de la ley así lo señala. Un servicio electrónico es la firma electrónica o la contratación electrónica, por ejemplo.

El primer inciso del artículo 21 del reglamento ut supra, determina que:

> “La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades (…)” (Reglamento a la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, art. 21).

La disposición del reglamento a la ley ibídem resulta muy restrictiva en cuanto a su ámbito de aplicación, ya que si no se trata de alguien que preste un servicio electrónico no tiene la obligación de cumplir lo dispuesto. Sin embargo es una disposición trascendente, pues consagra el deber de informar como uno de los pilares para el desarrollo del principio de seguridad en el tratamiento de los datos personales.

Tratándose de las bases de datos en poder del Estado, las disposiciones sobre medidas de seguridad derivan de las resoluciones de la Dirección Nacional de Registro de Datos Públicos (DINARDAP). La DINARDAP ha intentado establecer para las bases de datos que forman parte del sistema nacional de registro de datos públicos, medidas de seguridad por la tenencia de los datos. Mediante Resolución No. 9 publicada en el Registro Oficial 740, de 6 de julio de 2012, se promulgó el Instructivo para el Manejo de Contraseñas para el Ingreso al Servicio de Dato Seguro, por el cual se regula el manejo de las contraseñas que va utilizar cada usuario para ingresar al servicio de dato seguro. Como medida de seguridad se indican las características que deben tener las contraseñas, el bloqueo cuando estas sean incorrectas, indicaciones cuando existe olvido o el usuario ha perdido la contraseña y el tiempo de utilidad de la contraseña (Dirección Nacional de Registro de Datos Públicos, 2012).

Mediante Resolución No. 4 publicada en el Registro Oficial 718, de 6 de junio de 2012, se promulga el Instructivo para el Uso de Hojas de Seguridad en los Actos de los Registros Mercantiles de Ecuador, que establece procesos relacionados al manejo de las hojas de seguridad que usan los registros mercantiles del país, estas hojas de seguridad manejan la información de los actos registrales de los usuarios (Dirección Nacional de Registro de Datos Públicos, 2012).

Una vez que se terminen las hojas de seguridad en stock para los registros mercantiles, según lo dispuso la DINARDAP mediante Resolución No. 9 del Registro Oficial 503, de 19 de mayo de 2015; se procederá a utilizar el módulo de seguridad electrónica instaurado por el Sistema Nacional de Registro

Mercantil, el cual reemplazará a las hojas de seguridad (Dirección Nacional de Registro de Datos Públicos, 2015).

Finalmente, la Resolución No. 6 publicada en el Registro Oficial 508, de 26 de mayo de 2015, puso en vigencia la Norma de Implementación del Esquema Gubernamental de Seguridad de la Información para el Registro de Datos Crediticios, el cual se basa en el Esquema Gubernamental de Seguridad de la Información (EGSI) para el registro de los datos crediticios. En el caso de este tipo de registros aparece la figura preponderante del Oficial de cumplimiento, quien formará parte del Comité de Gestión de Seguridad de la Información de la Dirección Nacional de Registro de Datos Públicos. El Oficial de cumplimiento realizará funciones que aseguren una buena ejecución de los procesos para la protección de los datos en ámbito crediticio. (Dirección Nacional de Registro de Datos Públicos, 2015).

En materia de Telecomunicaciones, el Acuerdo Ministerial No. 32 publicado en el Registro Oficial 535, de 2 de julio de 2015, establece el uso de las aplicaciones DATO SEGURO, INFODIGITAL, el Sistema de Notificaciones Electrónicas (SINE) y de todas que son parte del Sistema Nacional de Registro de Datos Públicos (SINARDAP). Esto dirigido para desarrollar y fortalecer la interoperabilidad gubernamental. El artículo 4 del Acuerdo Ministerial referido, determina que la DINARDAP debe adoptar medidas apropiadas de seguridad para garantizar la protección de datos de carácter personal.

Por último, como análisis de algunas de las disposiciones legales en Ecuador, es importante hacer referencia también al Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos que se publicó mediante Decreto Ejecutivo en Registro Oficial 718 de 23 de marzo de 2016, en su art. 13, el cual señala que. En esta disposición se establece claramente que la Dirección Nacional de Registro de Datos Públicos determinará las normas técnicas que contengan los estándares y herramientas para la seguridad de la información, sin embargo es pertinente que se establezca clara y específicamente los mecanismos y estándares que se utilizarán, problema que se presenta en general, dentro del marco legal ecuatoriano.

Pues bien, teniendo en cuenta que existe variedad de disposiciones legales que hacen referencia a las medidas de seguridad en la protección de datos personales, y al haber determinado algunas de ellas en la normativa ecuatoriana, es preciso hacer un análisis de los puntos clave de las mismas y los vacíos que se presentan. Empezando con el artículo 21 del Reglamento a la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos en el que se menciona la seguridad en la prestación de servicios electrónicos, no se establece específicamente los parámetros o medidas de seguridad que se emplearán y aquello deja un vacío dentro de la norma. Por otra parte en la Resolución 9 de la DINARDAP, que hace mención al Instructivo para el Manejo de Contraseñas para el Ingreso al Servicio de Dato Seguro, las medidas de seguridad adoptadas están enfocadas al buen uso y función de las contraseñas de cada usuario, es decir a las indicaciones que deben acatar las personas que ingresen al portal, y de esta manera precautelar su información y evitar que sea violentada; por lo tanto se estipula de cierta manera parámetros o medidas de seguridad. En la Resolución 4 de la DINARDAP, sobre el Instructivo para el Uso de Hojas de Seguridad en los Actos de los Registros Mercantiles de Ecuador, presenta como una herramienta de seguridad el diseño y las características de seguridad tales como sellos, marcas, contraste y tipo de papel de las hojas de seguridad, como también las directrices de seguridad para dichas hojas, tales como el debido almacenamiento, custodia o anulación de las mismas. Como complemento a esta resolución se determina que si las hojas de seguridad se terminan se utilizará el módulo de seguridad electrónica instaurado por el Sistema Nacional de Registro Mercantil, el cual reemplazará a las hojas de seguridad. En la Norma de Implementación del Esquema Gubernamental de Seguridad de la Información para el Registro de Datos Crediticios que se encuentra establecido en la Resolución 6, enfoca la seguridad a la buena ejecución de los protocolos y procesos relacionados con la protección de la información crediticia, pero nuevamente no se determina de forma específica cuales serán estos procesos o protocolos que se utilizarán. En materia de telecomunicaciones tampoco se establece claramente las medidas de seguridad aplicables.

En general se puede constatar que hay varias inconsistencias y vacíos en las disposiciones legales ecuatorianas respecto al tema de medidas de seguridad. En unos casos no se especifican las medidas de seguridad que deben ser adoptadas y en otros se presentan como lineamientos muy simples de seguridad que no garantizan un adecuado y eficaz sistema de seguridad, ya que puede ser vulnerado.

A manera de colofón es importante destacar, que la inexistencia de normativa secundaria específica que desarrolle el derecho constitucional a la protección de datos, ha generado una dispersión normativa. En materia de seguridad en el tratamiento de datos personales, las diferentes disposiciones existentes en el ordenamiento jurídico ecuatoriano, resultan insuficientes y de aplicación parcial, lo que constituye un riesgo para la garantía del derecho constitucional referido.

CONCLUSIONES

El derecho a la protección de datos personales constituye el eje fundamental para garantizar el control y buen manejo de la información personal de cada individuo, ya sea dentro del ámbito público como del privado; los encargados o responsables de las bases de datos deben estar siempre alertas y utilizar los mecanismos o herramientas necesarias para que este derecho prevalezca en todo momento.

La seguridad en la protección de datos se muestra como el elemento más trascendente dentro de éste régimen y se configura en base al principio de seguridad. La legislación española y la legislación mexicana muestran diferentes puntos de vista en cuanto a cómo se deben estructurar las medidas de seguridad y qué tipo de medidas de seguridad pueden aplicarse. La legislación española clasifica a las medidas en nivel alto, mediano o bajo, que se deberán adoptar según el tipo de datos que se va a resguardar. Mientras que la legislación mexicana establece un sistema de gestión de seguridad para los datos personales. Cualquiera que fuese el caso, el objeto principal de las medidas de seguridad es el mismo: la protección de la información personal cuando es recopilada y transmitida, y que se encuentre en las bases de datos de una entidad, empresa, institución, etc.

Si bien en Ecuador existen normas, resoluciones y dictámenes que tratan sobre protección de datos personales en diferentes sectores como las telecomunicaciones, crediticios, salud, entre otros; no existe una ley de protección de datos. Esta realidad crea una dispersión normativa, de conceptos y preceptos que torna muchas veces compleja la ejecución y el procesamiento en el tratamiento de los datos. Para este régimen de protección de datos en general y sobre todo para la seguridad en la protección de datos personales, sería recomendable y apropiado que en Ecuador existiese una ley que regule todo lo relacionado a la protección de datos personales, que pueda mostrar de forma clara y concisa lo que conlleva la protección de datos en la normativa nacional, que establezca parámetros acorde a la realidad jurídica de nuestro

país y al progreso e importancia de este derecho estipulado en la Constitución de 2008 como un derecho de libertad de las personas.

REFERENCIAS

Alcaldía de Bogotá, (2012). *Ley Estatutaria de Protección de Datos Personales 1581*. Recuperado el 01 de agosto de 2016 de www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Agencia Española de Protección de Datos. (2016). *Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Recuperado el 28 de marzo de 2016 de https://www.agpd.es/portalwebAGPD/.../legislacion/.../directivas/index-ides-idphp.php

Agencia Española de Protección de Datos. (2016). *Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*. Recuperado el 30 de abril de 2016 de https://www.agpd.es/portalwebAGPD/canaldocumentacion/.../index-ides-idphp.php

Altmark, D. y Molina, E. (1998). *Informática y Derecho: Régimen jurídico de los bancos de datos*. Buenos Aires, Argentina: Depalma.

Blanco, M. (2015). *Protección de Datos Personales. Principios básicos de la protección de datos*. (1a. ed.). Madrid, España: Caecid.

Cámara de Diputados del Honorable Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Recuperado el 25 de mayo de 2016 de www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Conde, C. (2005). *La Protección de Datos Personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid, España: Dykinson.

Constitución de la República del Ecuador, Registro Oficial 449 de 20 de octubre de 2008.

Carbajal, L. (julio, 2005). La protección de datos personales y su necesaria incorporación en los ordenamientos jurídicos de América Latina. *Revista de Derecho Informático*. 84: Alfa-Redi.

Davara, M. (2008). *Manual de Derecho Informático*. (10a. ed.). Navarra, España: Aranzadi.

Dirección Nacional de Registro de Datos Públicos. Resolución No. 9 de Registro Oficial 740 de 6 de julio de 2012.

Dirección Nacional de Registro de Datos Públicos. Resolución No. 4 de Registro Oficial 718 de 6 de junio de 2012.

Dirección Nacional de Registro de Datos Públicos. Resolución No. 9 de Registro Oficial 503 de 19 de mayo de 2015.

Dirección Nacional de Registro de Datos Públicos. Resolución No. 6 de Registro Oficial 508 de 26 de mayo de 2015.

Dirección Nacional de Registro de Datos Públicos. Resolución 007-NG-DINARDAP-2014.

Dirección Nacional de Registro de Datos Públicos. Resolución 007-NG-DINARDAP-2014 (Anexo B).

Fernández, J. (2005). *Tecnologías de la Información. Aspectos Jurídicos*. Madrid, España: Davara & Davara.

Galindo, F. (1998). *Derecho e Informática*. Madrid, España: La Ley- Actualidad.

Guerrero, J. (2011). *La Ley del Sistema Nacional de Registro de Datos Públicos: Desafíos para la protección de datos*. Ponencia presentada en el XV Congreso Iberoamericano de Derecho Informático realizado en Buenos Aires.

Guerrero, M. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Navarra, España: Aranzadi.

Guibourg, R., Alende, J. y Campanella, E. (1996). *Manual de Informática Jurídica*. Buenos Aires, Argentina: Astrea.

Hassemer, W. y Chirino, A. (1997). *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.* Buenos Aires, Argentina: Editores del Puerto.

Herrán, A. (2003). *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao, España: Universidad de Deusto.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2013). *Recomendaciones en Materia de Seguridad de Datos Personales*. Recuperado el 25 de mayo de 2016 de www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.

León, W. (2001). De la comunicación a la informática: jurídica, penal, bancaria. Bogotá, Colombia: Ediciones Doctrina y Ley Ltda.

Lexis, (2016). Acuerdo Ministerial No. 32 de Registro Oficial 535 de 2 de julio de 2015. Recuperado el 5 de agosto de 2016 de www.lexis.com.ec/

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro Oficial 557 de 17 de abril de 2002.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Registro Oficial 52 de 22 de octubre de 2009.

Ley Orgánica de Telecomunicaciones. Registro Oficial 439 de 18 de febrero de 2015.

Ley de Propiedad Intelectual. Registro Oficial 426 de 28 de diciembre de 2006.

Ley del Sistema Nacional de Registro de Datos Públicos. Registro Oficial 162 de 31 de marzo de 2010.

Martínez, R. (septiembre, 2007). El derecho fundamental a la protección de datos: perspectivas. *Revista de Derecho y Política*.

Ministerio de la Presidencia de España. (2008). *Reglamento de desarrollo de la Ley Orgánica 15/1999*. Recuperado el 7 de mayo de 2016 de https://www.boe.es/buscar/act.php?id=BOE-A-2008-979.

Páez, J. y Acurio, S. (2010). *Derecho y nuevas tecnologías*. Quito, Ecuador: Corporación de Estudios y Publicaciones.

Pampillo, J. y Munive, M. (Coords.). (2012). *Derecho Informático e Informática Jurídica*. México D.F., México: Porrúa.

Peña, D. (2007). *Sociedad de la Información Digital: perspectivas y alcances*. Bogotá, Colombia: Universidad Externado de Colombia.

Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro Oficial 735 de 31 de diciembre de 2002.

Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos. Registro Oficial 718 de 23 de marzo de 2016.

Reglamento para Interoperabilidad de Información de Identificación. Resolución del Registro Civil No. 307 de 28 de junio de 2013.

Sánchez, A. (1998). *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla, España: Universidad de Sevilla, Secretariado de Publicaciones.

Santos, D. (2005). *Nociones Generales de la Ley Orgánica de Protección de Datos*. Madrid, España: Tecnos.

Serrano, M. (2003). *El derecho fundamental a la protección de datos. Derecho Español y comparado*. Madrid, España: Civitas.

Téllez, J. (2004). *Derecho Informático*. (3a. ed.). Monterrey, México: McGraw-Hill Interamericana.

Uicich, R. (1999). *Los bancos de datos y el derecho a la intimidad*. Buenos Aires, Argentina: AD-HOC S.R.L.

Universidad de los Andes. (2003). *Derecho de Internet & Telecomunicaciones*. Bogotá, Colombia: Legis.

Yánez, P. (1999). *Introducción al estudio del Derecho Informático e Informática Jurídica*. Quito, Ecuador: Escuela Politécnica Javeriana del Ecuador.