UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA

UNAN-LEON

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES

LA PROTECCION DE DATOS PERSONALES EN NICARAGUA

MONOGRAFIA PARA OPTAR AL TITULO DE LICENCIADOS EN DERECHO

AUTORES:

ERIC JAVIER FLORES BARRERA

WILLIAM LENNIN FLORES PEREZ

JONATHAN RAFAEL GONZALEZ ESPINOZA

TUTOR: Dr. Omar García Palacios. Ph.D.

León, Nicaragua Septiembre de 2014

“A la Libertad por la Universidad”

DEDICATORIA

Primeramente quiero dedicar esto a Dios ya que esto es obra de su voluntad, amor y misericordia.

A mi padre Enrique José Flores Castillo (Q.E.P.D) quien me enseño la importancia de aprovechar las oportunidades en la vida y que en ella nada bueno llega sin esfuerzo, sacrificio y disciplina, a mi madre Nydia Barrera de Flores quien siempre me ha impulsado a ser mejor persona cada día.

A mis hermanos, en especial a mi hermana por el apoyo incondicional que siempre me ha brindado.

A mi esposa y a mi hijo que han sido mi inspiración y motivación para avanzar en la vida y por ser las personas a las que quiero sientan mayor orgullo de mi persona.

Y por ultimo pero no menos importante al Msc. Juan Pablo Medina Rojas quien más allá de ser mi maestro y gran amigo ha sido un mentor para mi persona.

Eric Javier Flores Barrera

AGRADECIMIENTO

Primeramente debo agradecerle a Dios por derramar su sabiduría y bendiciones sobre mí.

A mis Padres ya que sin ellos nada de esto sería posible, a mi abuela, hermanos, tíos y primos quienes han sido de vital apoyo en mi formación, a nuestro tutor Dr. Omar A. García Palacios por compartir con nosotros sus conocimientos y guiarnos en esta etapa final de nuestra carrera.

En fin a todas las personas que a lo largo de mi vida me han rodeado y de una u otra manera han incidido en ser la persona que soy hoy en día. Gracias a todos.

Eric Javier Flores Barrera

DEDICATORIA

A dios y la virgen santísima quienes fueron y serán mis maestros por excelencia en toda mi vida.

Dedico este logro a mis padres Denis Flores y Josefa de los Ángeles Pérez que aun no estando conmigo en presencia física siempre fueron los mejores concejeros en los momentos difíciles de la vida y de esta manera cumplirles con lo prometido en el último momento de su vida.

A mis hermanos Carlos y Mariano Flores Pérez que siempre puedo contar con ellos para cualquier situación de mi vida.

En especial a mi hermana Aracely Bonilla Pérez por apoyarme en todo momento y ser quien me apoyo en toda la etapa universitaria y darme los mejores concejos que una hermana te puede dar en momentos de adversidad.

A mis Abuelos, a mis tíos y primos que siempre me motivaron en los momentos difíciles.

A mis Sobrinos Gedwin Denisse Flores y Carlos Fernando peralta Bonilla para que aun pasando todo tipo de problemas sigan siempre adelante confiando en dios que todo se lo resolverá.

Por eso hoy digo;

"TODO LO PUEDO EN CRISTO QUE NOS FORTALECE"

William Lennin Flores

AGRADECIMIENTO

Primeramente Doy infinitas gracias a Dios Todo Poderoso por haberme prestado la vida y así llegar a culminar esta etapa importante de la vida.

A nuestro Tutor Omar García Palacios por no escatimar esfuerzo y transmitirnos todos sus conocimientos sin reserva alguna.

A todas las personas que de una u otra manera me apoyaron en los momentos más difíciles que pude pasar en este largo camino de la vida.

William Lennin Flores

DEDICATORIA

Al Abogado por excelencia, Dios.

A mi leona de tiempo completo mi mama mi yunta mi estrella y mi amor, mama lo logre.

A mi papa Rafael González, por ser un ejemplo en mi vida por enseñarme a tener fe y seguir los sueños.

A mis hermanitas Gaby, Ninin y mi Nela.

A mi sobrina que espero que algún día tenga la oportunidad de leer esto, Estrellita Te Amo mucho.

A mis hermanos Yael, David, con los cuales sé que cuento para lo que sea.

A mis amigos de universidad, Mario Espino, Miguel Hernández, y compañía.

A Mayrita y a Karen dos buenas amigas, se les quiere mucho.

A mi tío Pedro Daniel Ocon González, por ser un ángel que vivió conmigo uno de los momentos difíciles de mi vida.

Esto es para todos ustedes, Gracias.

Jonathan Rafael González Espinoza.

AGRADECIMIENTOS

Al señor Dios todopoderoso por permitirme terminar una etapa de mi vida, por darme la sabiduría y rodearme buenos amigos durante este trayecto.

A mis padres, un ejemplo para mí.

A mis compañeros de monografía William y Eric los cuales compartimos buenos tiempos.

A nuestro tutor Omar García, por su tiempo y conocimientos compartidos.

En fin a todas las personas que Dios me puso en el camino para ayudarnos de una u otra manera, ustedes tienen una parte en este trabajo.

Jonathan Rafael González Espinoza.

Índice:

INTRODUCCIÓN.....1

CAPITULO I: ANTECEDENTES HISTORICOS, ACTUALIDAD Y DOCTRINA DE LA PROTECCION DE DATOS PERSONALES.....6

1.1 Generalidades y Antecedentes Históricos.....6

1.2 Etimología de Habeas Data.....9

1.3 Concepto de Habeas Data.....10

1.4 Tipos de Habeas Data.....11

1.5 Objeto.....14

1.6 Naturaleza.....15

1.7 Fundamento.....15

CAPITULO II: LA PROTECCION DE DATOS PERSONALES EN LA LEGISLACION COMPARADA.....17

2.1 La Protección de Datos Personales en Colombia.....17

2.1.1 Generalidades y Antecedentes.....17

2.1.2 Protección de Datos Efectiva.....18

2.1.3 Contenidos mínimos del recurso de Habeas Data.....21

2.2 La Protección de Datos Personales en Panamá.....22

2.2.1 Generalidades.....22

2.2.2 Tipos de Datos a los que se Puede Tener Acceso en la Legislación Panameña.....25

2.2.3 En lo que respecta a los tipos o clases de Hábeas Data.....28

2.2.4 En cuanto a lo que motiva la acción de Hábeas Data.....29

2.2.5 En lo que respecta al funcionario o persona contra la cual se promueve la acción de Hábeas Data.....30

2.2.6 Del tribunal competente para conocer del Hábeas Data.....30

2.2.7 En cuanto a la vía o formalidades para promoverla acción de Hábeas Data.....31

2.2.8 En cuanto al proceso al que da lugar la acción de Hábeas Data 32

2.3 La Proteccion de Datos Personales en Guatemala 33
2.3.1 Definiciones 33
2.3.2 Habeas Data en Guatemala.....34
2.3.3 Recurso de Revision 37
2.4 La Protección de Datos Personales en Costa Rica.....39
2.4.1 Generalidades.....39
2.4.2 Objeto 39
2.4.3 Definiciones 39
2.4.4 Principios 41
2.4.5 Tratamiento de los Datos.....42
2.4.6 De la Agencia de Protección de Datos de los Habitante (PRODHAB) 43
2.4.7 Procedimiento Realizado ante la PRODHAB 44
2.4.8 Procedimiento Sancionatorio.....45
2.4.9 Sanciones y Faltas 46
CAPITULO III: LA PROTECCION DE DATOS PERSONALES EN EL ORDENAMIENTO NICARAGUENSE.....48
3.1 Definición.....48
3.2 Naturaleza 49
3.3 Objeto 50
3.4 Sujetos.....50
3.5 Legitimación Procesal.....51
3.5.1 Legitimación Activa 51
3.5.2 Legitimación pasiva.....51
3.6 Procedimiento.....52
3.7 Procedimientos de inspección de ficheros.....55
3.8 Infracciones, Sanciones y su Procedimiento 58
3.9 Recurso de Habeas Data.....61
3.9.1 Motivación del Recurso 62
3.9.2 Interposición del Recurso y Tribunal Competente 62

3.9.3 Sentencia y sus Efectos.....65
CONCLUSIONES.....66
RECOMENDACIONES.....68
BIBLIOGRAFIA.....69
ANEXOS.....71

INTRODUCCIÓN

Los constitucionalistas dan el nombre de garantía a muchos de los preceptos contenidos en las declaraciones constitucionales, particularmente a los de caracteres objetivos, como por ejemplo: Articulo 32 de la Constitución "Ninguna persona está obligada a hacer lo que la ley no mande, ni impedida de hacer lo que ella no prohíbe". Articulo 36 Cn "Toda persona tiene derecho a que se respete su integridad física, psíquica y moral. Nadie será sometido a torturas, procedimientos, penas ni a tratos crueles, inhumanos o degradantes. La violación de este derecho constituye delito y será penado por la ley".

La representación que da vida al moderno constitucionalismo expresa por si misma las líneas generales de las garantías constitucionales que en su manifestación simplista, expresa una doble acepción. Por un lado, se entiende por garantía constitucional, la que reconoce el poder soberano, las libertades y sus diversos sectores, es decir, las públicas, civiles y políticas, para que puedan desenvolverse en la vida social; otras veces la acepción es restringida ya que se refiere únicamente a las libertades públicas. Pero para que las libertades públicas no pierdan su ritmo es necesario que el pensamiento pueda emitirse sin la injerencia del poder, lo que significaría que la representación política alcanza el mayor grado de perfección y las responsabilidades de los funcionarios son cada vez más exigentes.

Las libertades civiles y públicas derivan sus conceptos de los supuestos primordiales de familia y sociedad en general, ya que las libertades civiles se inician con las ideas supremas de la inviolabilidad personal, se desenvuelve en diversos aspectos que se producen tanto en la inviolabilidad del domicilio, del trabajo, de la propiedad, como del estado familiar.

Es un hecho que debido al avance tecnológico y la necesidad de los seres humanos de proteger el derecho a la intimidad y el derecho al buen nombre se han consagrado en la mayoría de los países del mundo como un derecho fundamental inherente al ser humano.

Inicialmente se consideró con la finalidad de proteger a las personas frente a datos o actos de índole personal que se ponían en conocimiento del público o de terceros sin el consentimiento y conocimiento del afectado.

Es ante este avance informático que aparece el Habeas Data el que nace con un sentido de protección del derecho a la intimidad dicho derecho tiene su origen en la Declaración Americana de Derechos y Deberes del hombre suscrita en Bogotá en 1948 y el pacto de San José Costa Rica; posteriormente en el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales realizado por el consejo de Europa en Roma el 14 de Noviembre de 1950, es hasta el año de 1970 que aparece la primera Ley un marco regulatorio para la protección de datos en el estado de Hesse Alemania, luego en 1973 se promulgo en Suecia la ley 289 con el objeto de prohibir la creación de registros de datos sensibles frente a las personas.

Debido a este problema es que toma capital importancia dentro del ordenamiento jurídico, la existencia del recurso de Habeas Data, el cual es visto como una garantía constitucional que protege el derecho a la intimidad en todos sus aspectos contra los atentados que a ella pudiera efectuar una persona individual o entidad pública o privada, pues la mayor parte de los países a nivel latinoamericano tanto como a nivel mundial ya cuentan con un mecanismo adecuado para la protección jurídica que evite la lesión a estos derechos.

La definición del Tema: La Protección de Datos Personales en Nicaragua represento el interés y el deseo de conocer a mayor profundidad el fenómeno

social y jurídico que compone el tratamiento de los datos personales de los individuos por parte de entidades públicas y privadas y como este tratamiento es regulado. Surgiendo de esta manera la interrogante que significa cuales son las semejanzas y diferencias entre las leyes que establecen mecanismos de protección a los datos personales en la región. Por otro lado el sometimiento a la crítica, el análisis y complementos son los instrumentos que ayudaron a resolver esta pregunta.

Mediante el uso de una investigación científica de carácter sistemático se propuso realizar esta tesis como una producción de conocimiento eminentemente básico. Esta investigación jurídica pretende explicar el tema definido en las distintas etapas que lo conforman prestando especial atención en su evolución.

La presentación de este trabajo de investigación es gracias a todos los conocimientos adquiridos a lo largo de nuestra formación universitaria permitiendo la exposición de su justificación, métodos aplicados, fuentes y la descripción de sus capítulos que a continuación se desarrollan.

Nos hemos planteado como objetivo principal Conocer la protección de datos personales y los procedimientos para su efectiva aplicación. Para complementar nuestro trabajo también tenemos como objetivos especificos señalar los antecedentes históricos de la protección de datos personales, estudiar los mecanismos de protección de datos en la legislación comparada y Determinar el procedimiento administrativo y jurisdiccional concerniente a la protección de datos personales en Nicaragua. La escasa publicación a nivel de tesis por parte del estudiantado en el área de la Protección de Datos Personales hizo que este trabajo estuviese motivado en abordar el tema de la protección de datos, especialmente en Nicaragua y la región ya que a pesar de ser un tema de interés es de poco conocimiento tanto para la población en general como en los lectores jurídicos interesados en el tema debido a la

novedad de este Derecho, debido a que existe información muy escaza en la publicación de las constituciones nacionales, tratados internacionales y leyes de esta índole propias de cada estado sin embargo careciendo de obras académicas especializadas en el derecho constitucional en materia de protección de datos personales esta tesis puede ser considerada como novedosa.

La principal importancia de este trabajo recae en la información brindada tanto en el contenido de sus capítulos como en la documentación aportada en sí misma. Permitiendo el análisis, comparación y reflexionar consecuentemente dejando abierta a las críticas y comentarios que estas puedan generar.

Esta obra pretenderá de un capitulo a otro exponer las principales ideas de manera breve y sencilla para su mejor información y comprensión por parte del lector.

Para cerrar esta sección es imperativo expresar la satisfacción que pueda esta obra tener para con su propósito de lectura general y/o búsqueda de tema especializado. No nos sirven las palabras para expresar el orgullo que para nosotros representaría que este trabajo sirva de guía para futuras investigaciones.

Se utilizó el método documental consultando tanto en libros físicos como en ediciones digitales, de diferentes autores especializados en temas, tesis y conferencias expuestas en organismos internacionales.

El método analítico fue empleado en la sustracción de las partes de un todo, con el objeto de estudiarlas y examinarlas por separado. Es así que se permite la mejor compresión entre temas y subtemas expuesto junto los conceptos y características, premisas.

El método comparativo recae en las similitudes y diferencias entras las legislaciones consultadas de las naciones mencionadas en la obra.

Las fuentes primarias fueron proporcionadas por las diferentes leyes que en Nicaragua regulan la materia así como leyes semejantes en los países incluidos en este estudio, destacando su importancia y funcionalidad.

Como fuente secundaria citamos a las obras publicadas por jurista y expertos en la materia de distintas universidades de Nicaragua, México y algunos autores centroamericanos.

En el desarrollo del primer capítulo se desarrolló el estudio de los antecedentes históricos así como la evolución del Habeas Data, su etimología, definición, objeto y tipos.

En el segundo capítulo se desarrolló el análisis las legislaciones comparadas en materia de protección de datos personales en las repúblicas de Colombia, Panamá, Guatemala y Costa Rica.

El tercer capítulo es el análisis de las normas jurídicas de carácter nacional, en las cuales destacamos los mecanismos para la protección de datos personales, procedimientos tanto administrativos como jurisdiccionales y los efectos que sus resoluciones producen.

CAPITULO I: ANTECEDENTES HISTORICOS, ACTUALIDAD Y DOCTRINA DE LA PROTECCION DE DATOS PERSONALES

1.1 Generalidades y Antecedentes Históricos

El derecho a la intimidad y el derecho al buen nombre se han consagrado en la mayoría de los países del mundo como un derecho fundamental inherente al ser humano. Inicialmente se consideró buscando proteger a las personas frente a datos o actos de índole personal, que se ponían en conocimiento del público o de terceros sin el consentimiento del afectado. Con la aparición de las tecnologías de la información y las comunicaciones aparece la necesidad de regular el manejo de la información electrónica que reposa en bases de datos sobre las personas, por lo tanto, la evolución histórica del "Habeas Data" inicia con un marcado sentido proteccionista del derecho a la intimidad progresando hacía un sistema legislativo donde se equilibre la protección de dicho derecho con la libertad de información.[1] A continuación se enuncian algunos hechos históricos sobre la evolución de dicho concepto.

En el año de 1948 se dieron los primeros antecedentes regulatorios en relación con la intimidad o la privacidad de las personas, en el marco de las Naciones Unidas: con la Declaración de los Derechos del Hombre que establece en el Artículo 12 que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[2]

[1] Evolución de la Protección de Datos, disponible en http://www.redipd.org/noticias-habeasdata. Consultada el 5 de Abril del 2014.
[2] Declaración Universal de los Derechos Humanos, 1948, Paris, Francia, art. 15.

En el mismo sentido, La Declaración Americana de Derechos y Deberes del Hombre suscrita en Bogotá en 1948 y el Pacto de San José de Costa Rica en su artículo 11 sobre la Protección de la Honra y de la Dignidad establece que "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."[3]

En 1966 El Pacto Internacional de Derechos Civiles y Políticos de Nueva York dictaminó en su artículo 17 que "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques." [4] Igualmente, empieza a aparecer también un reconocimiento expreso al derecho a la información, cuando señala en su artículo 19 numeral 2º que "Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección."[5]

En el Consejo de Europa, el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales realizado en Roma el 14 de noviembre de 1950, en su artículo 8 numeral 1 establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y

[3] Convención Americana Sobre Derechos Humanos, 1969, San José, C. R., art. 11.
[4] Pacto Internacional de Derechos Civiles y Políticos, 1966, Nueva York, EUA, art. 17.
[5] Ver Pacto Internacional de Derechos Civiles y Políticos, art. 19 numeral 2.

correspondencia".[6] Observándose el respeto de la vida privada y familiar de las personas.

En 1970 aparece la primera ley que estableció un marco regulatorio para la protección de datos, en el Estado de Hesse Alemania, en donde se creaba un Comisario Parlamentario de protección de datos para velar por la confidencialidad en el manejo de los datos de los particulares.

En 1973 se promulgó en Suecia la ley N. 289, prohibiendo la creación de registros de datos sensibles frente a las personas. En el mismo año se promulgó por el Consejo de Europa la resolución 29 que fijó pautas para la protección de datos en el sector público y se detallaron los principios básicos de operación de datos, como el de exactitud, finalidad y licitud en la obtención de la información, el derecho al acceso por parte del ciudadano, el régimen estricto de conducta para quienes operan la información y la aplicación de mínimos de seguridad.

En 1974 se llegó a la "Privacy Act" norteamericana, que buscaba proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado. En 1976 La Constitución de Portugal les da derecho a las personas a informarse sobre los contenidos de los bancos de datos que le conciernen y sobre el uso que se le pretendan dar a los datos. En 1977 se aprobó en Alemania la primera ley Federal de Protección de Datos que organizaciones públicas y privadas manejaban de las personas. En 1978 se promulgó en Francia la ley de Informática, Ficheros y Libertades, que se encuentra aún vigente.

[6] Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, 1950, Roma, Italia, art. 8 numeral 1.

En 1978 la Constitución Española en su artículo 18 numeral 4 establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[7] En 1981 se aprobó la Data Protection Act, ley de protección de datos del Reino Unido, que se caracteriza por el registro de un operador para manejar la información de las personas previo registro ante un registrador gubernamental creado por la ley.

1.2 Etimología de Habeas Data

El término "Hábeas" proviene de los orígenes latinos "Habeo" o "Habere", cuyos múltiples significados son: tener, poseer, gozar, disfrutar, exhibir, presentar, tomar, aprehender, traer, trasladar, transportar, entre otros términos sinónimos. Por su parte "Data" proviene del latín "datum" que significa dato, igualmente es un sustantivo plural anglosajón y que significa información o datos, en relación con lo que se pretende tutelar o proteger. En síntesis su traducción textual sería "conserva o guarda los datos".[8]

El concepto de datos, es definido como el antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho. En un ámbito más sistemático, el dato es el elemento básico de la información, conformado entre otros por letras, números, dibujos, señas, gestos; que asociado llegan a cobrar sentido.[9]

En la legislación nacional vigente se entiende por datos personales toda información que se tenga sobre una persona sea esta natural o jurídica que la identifica o la hace identificable. Además, que estos a su vez los clasifica en datos personales informáticos los cuales son los tratados por medio de

[7] Constitución Española, 1978, Madrid, España, art. 18 numeral 4.
[8] Definición de Habeas Data, disponible en http://www.mediawix.com/proteccion_de_datos_personales. Consultada el 13 de Marzo del 2014
[9] Diccionario de la Real Academia de la Lengua Española, disponible en http://www.rae.es/rae.html. Consultado el 1 de Marzo de 2014.

medios electrónicos automatizados, y datos personales sensibles que es toda información que revele el origen racial, étnico, filiación política, antecedentes penales o faltas administrativas. Así como información crediticia y financiera, etc.

También hay que tener presente las demás definiciones que nos refleja la norma específica sobre los ficheros de datos que son los archivos, registros, bases o bancos de datos que contienen de manera organizada los datos personales, automatizados o no. La disociación de datos que no es más que el tratamiento de datos personales de tal manera que la información obtenida no pueda asociarse a persona determinada.

Por lo tanto el "Habeas Data" se entiende como el derecho que tienen las personas a solicitar la exposición de datos en los cuales está incluido, a fin de tomar conocimiento de su veracidad, sea para rectificarlos o para suprimirlos en caso de ser haber cambiado, si son inexactos o falsos.

1.3 Concepto de Habeas Data

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

Alfredo Chirino lo define como "una garantía o mecanismo jurídico procesal que permite la defensa, la realización de derechos fundamentales, en este caso, el derecho a la intimidad, a la autodeterminación informativa contra el uso indebido por parte de terceras personas".[10]

[10] Hassemer, Winfried, Proteccion de Datos Personales, Editores del Puerto, Buenos Aires, Argentina, 1997, P. 28.

Para Rubén Flores Dapkevicius el Habeas Data es una garantía de tercera generación en tanto protege algunos derechos que han evolucionado, y que pueden definirse como aquellos que intrínsecamente son, a la vez, individuales y colectivos.[11]

Por último, en nuestra legislación el Doctor Iván Escobar Fornos define el Habeas Data como un proceso constitucional que se inicia con la acción que le asiste a toda persona para solicitarle a las autoridades judiciales la exhibición de los registros que llevan las autoridades o las personas privadas en los cuales aparecen sus datos personales o las de su grupo familiar o étnico para que se las exhiban, enterarse de su exactitud y de la razón de su existencia, y pedir su rectificación, supresión o modificación si fueren inexactos o encierren una discriminación.[12]

1.4 Tipos de Habeas Data

- **El Habeas Data Informativo:**

Es aquel que se orienta solamente a conseguir información accediendo a registros o bancos de datos públicos o privados; regulado por la constitución Política Colombiana en el artículo 15. Dentro de este tipo encontramos a su vez a tres subdivisiones.[13]

- **El Habeas Data Exhibitorio:**

Se ejercita con la finalidad que el titular de los datos, pueda tener conocimiento integral acerca de los datos que se almacena en determinado registro, de manera que por este medio la persona tiene derecho a controlar

[11] Flores Dapkevicius, Rubén, Amparo, Habeas Corpus, Habeas Data, Editorial BDF, Buenos Aires, Argentina, P. 60.
[12] Escobar Fornos, Iván, Introducción al Derecho Procesal Constitucional, Editorial Porrúa, México D. F., P. 300.
[13] Pucinelli, Oscar Raúl, Variaciones, Tipos y Subespecies del Habeas Data en el Derecho Latinoamericano, Revista Iberoamericana de Derecho Procesal Constitucional, Numero 1, Enero – Junio 2004 Pág. 93 y sigs. Disponible en www.justiciayderecho.org/revista3/articulos/09%20Modalidades%20/%subtipos.pdf consultada el 25 de Marzo del 2014.

que datos acerca de ella están contenidos o incorporados a un registro o base de datos.[14]

- **El Habeas Data Finalista:**

Permite saber con qué finalidad los datos se encuentran archivados en determinada base y para qué entidad o que persona o personas fueron registrados.[15]

- **El Habeas Data Autoral:**

Sirve para saber quién fue el agente que actuó como autor o la fuente de la que provino la captación de los datos insertados o contenidos en el registro, en tal sentido se persigue establecer la fuente u origen, es decir quién es la persona que recopiló, captó, o suministro la información que ingreso al registro. [16]

- **El Habeas Data Aditivo:**

Mediante este tipo de "Habeas Data" el interesado reclama ante el responsable de administrar la información, por alguna omisión, de manera que su pretensión tiene por finalidad el que se agregue otros datos adicionales a los que ya figuran en el registro respectivo. Es esta clasificación se tienen 3 subdivisiones.[17]

- **El Habeas Data Actualizador:**

Diseñado para actualizar datos, pues los que están actualmente no corresponden al estado actual de las cosas.[18]

[14] idem
[15] idem
[16] idem
[17] idem
[18] idem

- **El Habeas Data Aclaratorio:**

Destinado a aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas por quien acceda a los datos contenidos en los registros o bases de datos.[19]

- **El Habeas Data Inclusorio:**

Cuya finalidad es la de operar sobre un registro que ha omitido asentar los datos del interesado, quien se encuentra perjudicado por dicha omisión.[20]

- **El Habeas Data Rectificador o Correctivo:**

Dirigido a la corrección de los errores, así como las imprecisiones que existen almacenadas en los registros, archivos, bancos o base de datos públicos o privados. Puede decirse que mediante esta modalidad se sanean los datos falsos. [21]

- **El Habeas Data Exclusorio o Cancelatorio:**

Pretende eliminar total o parcialmente los datos almacenados respecto de determinada persona, cuando por algún motivo no deben mantenerse incluidos en el sistema de información de que se trate. Ello puede ocurrir en múltiples supuestos, como en el caso del registro de cualquier tipo de datos que no se correspondan con la finalidad del banco o base de datos, de datos falsos que el registrador se niega a rectificar o actualizar.[22]

- **El Habeas Data Reservador:**

[19] idem
[20] idem
[21] idem
[22] idem

El objetivo es mantener en reserva los datos de la persona que se encuentran registrados en la base o banco de datos; la finalidad que se persigue en esta modalidad a diferencia de las otras, es que no sirve para adicionar, incluir, ni para rectificar errores; sino para mantener la privacidad, el secreto y la reserva de los datos. Según Puccinelli, se trata de una modalidad cuyo fin es asegurar que un dato legítimamente registrado sea proporcionado solo a quien se encuentran legalmente autorizados para ello.[23]

1.5 Objeto

Este tipo de recurso constitucional tiene un amplio objeto, el cual es el de proteger los datos de cada una de las personas, el cual seguirá evolucionando de acuerdo a las necesidades de la sociedad y el avance tecnológico ya que por medio de este los individuos tienen el derecho de poder acceder a la información que sobre él se tenga en registros o bancos de datos de las entidades sean estas públicas o privadas[24,] así como también el derecho de exigir la actualización o rectificación de les datos que sobre él se tengan registrados y de esta manera se asegura la confidencialidad y no divulgación de dicha información a terceros, como el derecho de pedir la supresión de la información sensible que exista sobre su persona en los bancos de datos[25], es debido a estas necesidades que nuestra legislación en nuestra Constitución política en su artículo 26 en el cual se reconoce el derecho a la autodeterminación informativa así como también lo reconoce en el artículo 1 de la ley 787 en la cual se reconocen los derechos y el tratamiento que los datos deben de tener por parte de las entidades públicas o privadas.

[23] idem
[24] Escobar Fornos, Iván, Ob Cit, P. 299.
[25] Flores Dapkevicius, Rubén, Ob Cit, P68.

1.6 Naturaleza

El habeas data tiene una naturaleza privada ya que este se deriva del derecho a una vida privada que tiene cada individuo y es un recurso de tercera generación que tiene por objeto la protección de los derechos humanos como son el derecho a la inviolabilidad del domicilio, de las comunicaciones, y también es considerado así por el doctor Rubén Flores Dapkevicius en su obra Amparo, Habeas Corpus y Habeas data en donde lo define como una garantía de tercera generación y por formar parte del denominado derecho procesal constitucional y como un instrumento procesal para la protección de determinados derechos humanos[26]. El doctor Iván Escobar Fornos coincide con Flores Dapkevicius en relación a la naturaleza privada al sostener que el habeas data deriva del derecho a una vida privada interna, íntima es decir es una parte sustancial del derecho a la intimidad, que se deriva a su vez del derecho a la dignidad.[27]

1.7 Fundamento

El Habeas Data tiene su fundamento en las necesidades de las personas de protegerse frente a la recolección y tratamiento de información personal la cual está viviendo en la actualidad un periodo de cambio profundo debido al acelerado desarrollo de la informática.

Esto es provocado por las nuevas formas tecnológicas de información, como las bases de datos, los correos electrónicos etc. Los cuales presentan una mayor rapidez e interconexión entre los registros y es por causa de este fenómeno que se han tenido que revisar de manera necesaria las normas vigentes para el manejo de documentos, ya que el acumular información y ofrecerla a terceros o publicarlas es un característica de esta época; no porque

[26] idem
[27] Escobar Fornos, Iván, Derecho Procesal Constitucional, la Constitución y su Defensa, Hispamer, Managua, 1999, P. 274.

la aspiración fuera novedosa, sino porque las modernas técnicas así lo permiten, tanto para la acumulación como para la divulgación.

Para el doctor Iván Escobar Fornos el fundamento jurídico de este recurso se debe a que el Habeas Data se deriva del derecho a una vida privada interna, íntima. Ya que es un parte sustancial del derecho a la intimidad, que se deriva a su vez del derecho a la dignidad.[28]

Sigue expresando el doctor Escobar Fornos que por ser el derecho a la intimidad, un derecho de amplio aspecto requiere de las protecciones e inviolabilidades de los Derechos Humanos como la inviolabilidad del domicilio, de las comunicaciones y sobre todo la protección frente a la informática que es el fenómeno que hoy nos aqueja en materia de datos personales[29], y éste derecho de protección de los datos personales o dicho de otra manera el derecho a una vida privada está consagrado en nuestra Constitución vigente en su artículo 26 numeral 1 y 4 el cual dice literalmente "toda persona tiene derecho: a su vida privada y la de su familia." "toda persona tiene derecho a conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tienen esa información".[30]

[28] idem
[29] Escobar Fornos, Iván, Introducción al Derecho Procesal Constitucional, Editorial Porrúa, México D. F., 2005, P. 302
[30] Constitución Política de la Republica de Nicaragua de 1987 y sus Reformas.

CAPITULO II: LA PROTECCION DE DATOS PERSONALES EN LA LEGISLACION COMPARADA

2.1 La Protección de Datos Personales en Colombia

2.1.1 Generalidades y Antecedentes

A partir de 1985 la mayoría de las constituciones de los países latinoamericanos han tratado los datos personales como una información protegida constitucionalmente. Paralelamente, las constituciones han conferido al titular del dato, derechos (acceso, corrección, actualización, supresión, eliminación o cancelación de información persona) y acciones constitucionales como el Habeas Data. No obstante, desde la óptica política existe un reconocimiento de su naturaleza como lo refleja el numeral 45 de la declaración de Santa Cruz de la Sierra, del 15 de Noviembre del 2003 en donde los asistentes Jefes de Estado y de Gobierno de Veintiún países Iberoamericanos manifestaron que "La protección de Datos personales es un derecho fundamental de las personas.

Es así, que en la década de 1990-2000 la Constitución Colombiana da los primeros pasos en materia de Protección de Datos, surgiendo de esta manera los primeros preceptos que permiten el ejercicio de estos derechos frente a entidades públicas y privadas, lo cual, lo estableció en su artículo 15 de la Constitución de 1991, en el cual se leía literalmente "Todas las personas tienen Derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de Datos al igual que en los archivos de entidades públicas y privadas."

Dicho artículo fue reformado mediante acto legislativo del 02 del 2003 que dice literalmente: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las

informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

2.1.2 Protección de Datos Efectiva

Con el fin de prevenir la comisión de actos terroristas, se crea una ley estatutaria (Ley 184 del 2010) la cual reglamentará la forma y condiciones en que las autoridades que ella señala específicamente, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Este artículo sufre una nueva reforma mediante sentencia C-816 del 2004 el cual dice literalmente "Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe

respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

"En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

"La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

"Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

"Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Debido a estas reformas que ha sufrido la Constitución Política Colombiana se le debe de dar una mención especial a la ley estatutaria 1266 aprobada el 31 de diciembre del año 2008, en la cual se establecen la disposiciones relativas al recurso de Habeas Data, y es bueno resaltar la sentencia C-784/11 del 6 de octubre del año 2011 de la corte constitucional en la cual se

lleva a cabo el control constitucional al proyecto de ley estatutaria número 184 del 2010 por medio de la cual se dictan disposiciones generales para la protección de datos personales.

Es importante señalar que la Corte Constitucional en la sentencia C-1011 de 2008 ha señalado que la Ley 1266 de 2008 no es una norma general sino una norma sectorial que rige el tratamiento de los datos sobre el cumplimiento e incumplimiento de las obligaciones dinerarias. Es decir, es una regulación del Habeas Data financiero y no del habeas data general por lo que se decide crear y aprobar la ley estatutaria 184 del 2010.

En la jurisprudencia constitucional, el derecho al Habeas Data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad. Según esta línea, el Habeas Data tiene su fundamento último en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad. Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al Habeas Data como un derecho autónomo, en que el núcleo del derecho al Habeas Data está compuesto por la autodeterminación informática y la libertad, incluida la libertad económica. Este derecho es fundamental y autónomo, es por esto que requiere para su efectiva protección, de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además

del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

2.1.3 Contenidos mínimos del recurso de Habeas Data

Del mismo modo, en dicha Sentencia (C-748 de 2011) se señalan los contenidos mínimos del derecho al Hábeas Data de la siguiente manera: Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al habeas data encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer acceso la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien por qué se está haciendo un uso indebido de ella, o por simple voluntad del titular salvo las excepciones previstas en la normativa

Igualmente en la sentencia C-748 de 2011 se condensan y consagran los puntos característicos e individualizadores de este derecho: “La jurisprudencia constitucional colombiana ha precisado que las características de los datos personales son las siguientes: i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita iv) su tratamiento está sometido a

reglas especiales (principios) en lo relativo a su captación, administración y divulgación".

2.2 La Protección de Datos Personales en Panamá

2.2.1 Generalidades

En la legislación panameña el Habeas Data se encuentra normado por la ley 6 del 22 de Enero del 2002, como es él siempre es el caso cada legislación le da un concepto distinto a lo que el Habeas Data consiste, en el caso de panamá el habeas data es la protección del derecho a la intimidad o a la no injerencia o conocimiento público, de aquellos datos denominados sensibles y que pueden verse manipulados en perjuicio de su titular, por el llamado poder informático.

Cabe señalar, en consecuencia, que en el sistema constitucional panameño se regulan los derechos que preservan aquella esfera de privacidad o de intimidad del individuo, dentro de la cual se busca impedir el que no sea objeto de intromisiones o injerencias lesivas a su imagen, a su honor y a su decoro.

Mediante la ley Nº 6 de 22 de enero de 2002, por la cual se adoptan las normas pertinentes "para la transparencia en la gestión pública", se vino a establecer o incorporar a este ordenamiento jurídico, la acción de Hábeas Data, con lo cual se ha venido a actualizar y a la vez reforzar, el sistema de garantías para la protección efectiva de los derechos fundamentales en Panamá

En lo que a la Ley 6 de 2002 concierne, cabe dejar señalado que ésta, además del Hábeas Data, se refiere a otros aspectos como lo son el reconocimiento del derecho al acceso a la información, ya sea ésta de carácter público como a los datos personales, la obligación que tiene el Estado de informar en

cuanto a su gestión, la información que es de carácter confidencial y la de acceso restringido, entre otras materias. Ello significa por ende, que se está ante una ley que conjuga diversos temas relacionados entre sí.

En cuanto al Hábeas Data, éste se regula en el Capítulo V, denominado "Acción de Hábeas Data", el cual abarca del artículo 17 al 19 inclusive, aunque otras normas fuera del aludido capítulo guardan relación con lo que en éste se prevé y a los que nos referimos en su momento.

Dispone el artículo 17 de la ley 6 de 2002, que:

"**Artículo 17**. Toda persona estará legitimada para promover acción de Hábeas Data, con miras a garantizar el derecho de acceso a la información previsto en esta Ley, cuando el funcionario público o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado, no le haya suministrado lo solicitado o si suministrado lo requerido se haya hecho de manera insuficiente o en forma inexacta".

Como se ve, en primer lugar, la acción de Hábeas Data podrá ser promovida "por toda persona" a la que no se le haya suministrado la información o dato personal solicitado o cuando se haya hecho de forma deficiente. Significa ello que ésta no está restringida solamente a los ciudadanos panameños, sino, como establece la norma, "a toda persona", sea ésta, entendemos nosotros, nacional o extranjera, persona natural o jurídica, claro, está de acuerdo a las restricciones que en la ley se señalan y según la información o dato personal que haya sido requerido.

Así, por ejemplo, en cuanto a la legitimación para poder solicitar y tener acceso a una información o dato que verse sobre una persona en particular, ya sea porque tenga que ver con una información o dato estrictamente personal, se entiende que sólo la persona cuya información o dato le

concierne, será a la que se le reconozca dicha legitimación y no a cualquier otra cuya información o dato personal no sea de su incumbencia.

Con relación a lo que se viene expresando, la ley 6 de 2002 dispone o determina que la información que tenga el carácter de confidencial, "no podrá ser divulgada bajo ninguna circunstancia, por agentes del Estado", lo que establece así el artículo 13 del texto legal en mención. En el numeral 5 del artículo 1 de la ley 6 en estudio, al definir lo que se entiende por Información Confidencial, deja establecido que ésta es:

"Todo tipo de información en manos de agentes del Estado o de cualquier institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. Para efectos de esta ley, también se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios."

Lo que ha de entenderse, en cuanto a la información así considerada, que a ésta no tendrá acceso cualquier persona o al ser dicha información confidencial le está prohibido a los agentes del Estado, divulgarla, pero en manera alguna se le podrá impedir o negar el acceso a la misma, a la persona a la que sí corresponda o concierna la información o dato personal así recabada y que reposa en archivos o está informatizada.

Por otra parte, en el numeral 7 del artículo 1 de la ley 6 de 2002, se define como información de acceso restringido, aquella que está "manos de agentes del Estado o de cualquier institución pública, cuya divulgación haya sido

circunscrita únicamente a los funcionarios que la deban conocer en razón de sus atribuciones, de acuerdo con la ley". Para que una información sea considerada como de acceso restringido, debe previamente ser declarada o calificada como tal por parte de funcionario competente, como lo deja establecido el artículo 14 de la ley en referencia, considerándose así, entre otra, la que tenga que ver con la seguridad nacional, manejada por los estamentos de seguridad, los asuntos que tengan que ver con procesos o sumarios que lleven a cabo el Ministerio Público y el Órgano Judicial, a los que sólo podrán acceder las partes del proceso, etc.

De acuerdo al citado artículo 14, la información definida como de acceso restringido, "no se podrá divulgar, por un período de diez años, contados a partir de su clasificación como tal, salvo que antes del cumplimiento del período de restricción dejen de existir las razones que justificaban su acceso restringido". Por consiguiente, y en base a lo que se lleva explicado, la acción de Hábeas Data no podrá promoverse por cualquier persona cuando de información confidencial se trate, ya que en este caso sólo estará legitimada la persona cuya información o dato personal le haya sido recabada y, cuando se esté ante información de acceso restringido no procederá por persona alguna esta acción, salvo que hayan transcurrido los diez años a los que puede estar sometida ésta sin permitir su divulgación o cuando las condiciones que motivaron dicha clasificación hayan dejado de existir.

2.2.2 Tipos de Datos a los que se Puede Tener Acceso en la Legislación Panameña

En el transcrito artículo 17 de la ley 6 de 2002, se establece que la acción de Hábeas Data es un mecanismo previsto con miras a garantizar "el derecho de acceso a la información" a la que se refiere la ley en mención y que la

misma procede cuando "la información o dato personal reclamado", no haya sido suministrado o lo haya sido en forma insuficiente o en forma inexacta.

Implicaría lo anterior que serían dos los tipos o clases de información a la que se tiene derecho a tener acceso. Uno vendría a ser la de carácter general y pública, es decir la que está en manos del Estado y la otra cuando tal información es de tipo personal, al tratarse de una información o dato que habiendo sido recabado por una entidad o institución pública, tiene que ver con una persona en particular.

La primera se entiende que debe ser de acceso de cualquier persona, sin tener que alegar o "sustentar justificación o motivación alguna", como lo tiene señalado el artículo 2 de la ley en estudio. La otra, a nuestra manera de entender, en la medida en que incumbe a una sola persona, por ser una información o dato personal, su acceso si bien no le estará vedado por tener derecho a conocer y tener control sobre la misma, lo que ya si no será permitido es que a ésta tenga acceso cualquier otra persona.

Por lo demás, a una y otro tipo o clase de información se refieren los artículos 2 y 3 de la ley 6 de 2002.

En ese sentido, el artículo 2 y al cual ya se hizo alusión, es del contenido siguiente:

"Artículo 2. Toda persona tiene derecho a solicitar, sin necesidad de sustentar justificación o motivación alguna, la información de acceso público en poder o en conocimiento de las instituciones indicadas en la presente ley.

Las empresas privadas que suministran servicios públicos con carácter de exclusividad, están obligadas a proporcionar la información que les sea solicitada por los usuarios del servicio, respecto de éste".

Por su parte, en el artículo 3 se establece que:

"**Artículo 3**. Toda persona tiene derecho a obtener su información personal contenida en archivos, registros o expedientes que mantengan las instituciones del Estado, y a corregir o eliminar información que sea incorrecta, irrelevante, incompleta o desfasada, a través de los mecanismos pertinentes".

Se sigue de las normas transcritas que la legitimación para presentar y promover la acción de Hábeas Data, va a tener que ver con:

a. La información de acceso público que esté o se encuentre en poder o de conocimiento de instituciones del Estado, las que incluyen toda agencia o dependencia de éste, ya sea que pertenezcan al Órgano Ejecutivo, Legislativo, Judicial, al Ministerio Público o de las entidades descentralizadas, autónomas o semiautónomas, la Autoridad del Canal, los municipios, gobiernos locales, los patronatos y los organismos no gubernamentales, en este último caso, cuando "hayan recibido o reciban fondos, capital o bienes del Estado", como se regula en el punto 8 de definiciones o términos del artículo 1 de la ley en estudio.
b. La información que esté en poder o haya sido recabada por las empresas que aunque privadas o particulares, suministran o llevan a cabo prestación de servicios públicos con carácter de exclusividad, caso en el cual la información que están obligados a proporcionar, será aquella que tenga que ver con la de los usuarios del servidor.
c. La información o dato personal que se haya recabado y que esté contenida en archivos, registros o expedientes que estando en instituciones del Estado, sea de índole personal y que atañe a quien la solicita o reclame.

2.2.3 En lo que respecta a los tipos o clases de Hábeas Data

En cuanto a esto concierne, cabe señalar que por el tipo o clase de información que da derecho a acceder por medio de la acción de Hábeas Data, tal y como quedó previsto en la ley 6 de 2002 y a lo que acabamos de referirnos, se ha dado cabida en nuestro ordenamiento , a las dos clases de Hábeas Data, a los que alude Oscar Puccinelli, al reconocer la existencia del Hábeas Data "tradicional" o "propio", por el cual se busca "mitigar los efectos perniciosos del poder informático sobre los derechos de las personas" y la otra modalidad lo sería el Hábeas Data "no tradicional" o "impropio", el que, a decir del citado autor, "se relaciona con la pretensión de tutelar la libertad de recabar y transmitir información (...), cuya misión es la de funcionar como mecanismo corrector de los abusos de quienes pretenden escatimar indebidamente el acceso a las fuentes de información (generalmente el Estado).

Así, a través del Hábeas Data propio se garantizará el acceso a la información o dato personal de quien la reclama y por ser de su incumbencia y por medio del impropio lo que se persigue es dotar a toda persona que así lo haya solicitado, el acceso a las fuentes de información de carácter público.

Se introduce y regula por tanto en nuestro sistema jurídico, un Hábeas Data amplio, al regularse éste en sus dos modalidades y por los cuales, tanto para la persona que solicita su información o dato personal, como para quien la que requiere es de índole general, se dota a uno y otro de un instrumento jurisdiccional que viene a poner freno y remedio a los caprichos y arbitrariedades de

Aquellos funcionarios públicos que, desconociendo el derecho que se tiene a la información por parte de toda persona, ya sea de acceso público o cuando

lo sea de carácter particular, se termina negando el conocimiento de la misma.

2.2.4 En cuanto a lo que motiva la acción de Hábeas Data

En el artículo 17 de la ley 6 de 2002, se deja establecido que el Hábeas Data se podrá promover cuando la información o dato personal, no se le haya suministrado a quien la requirió o se suministró en forma insuficiente o de manera inexacta.

Como se ve, tres van a ser los supuestos que de darse traerán como consecuencia el que se pueda promover el Hábeas Data, a saber:

a) Cuando ante la solicitud de una información, sea ésta de acceso público o de carácter personal, el funcionario titular o responsable del registro, archivo o banco de datos, no haya suministrado lo solicitado,
b) Cuando pese a que lo requerido se suministró, lo fue de forma insuficiente,
c) Y cuando la información o dato ya sea público o de carácter personal no es exacta o no corresponde a una información o dato correcto o ajustado a la verdad.

Tanto en un caso como en los otros, lo que viene a fundamentar en última instancia el que se formule el Hábeas Data, es la violación, desconocimiento o menoscabo del derecho que se tiene de acceso a la información o dato personal. Como tal infracción es lesiva al derecho así reconocido, es por lo que requiere se le brinde la tutela necesaria y efectiva a través de un mecanismo jurisdiccional, lo que se logra con la acción de Hábeas Data.

2.2.5 En lo que respecta al funcionario o persona contra la cual se promueve la acción de Hábeas Data

La acción de Hábeas Data tendrá como funcionario demandado, en primer lugar, el que es "titular o responsable del registro, archivo o banco de datos" en el que se encuentra o se halla la información o dato personal requerido, según sea el caso. De manera que reconocido el "derecho que tiene toda persona para solicitar y recibir información veraz y oportuna, en poder de las autoridades gubernamentales y de cualquier institución" y en especial cuando se trate de "información personal" de quien la reclama, ante el incumplimiento de proporcionar ésta o cuando se haya suministrado de manera insuficiente o de forma inexacta, se promoverá acción de Hábeas Data contra el funcionario que es el responsable de suministrar o permitir el acceso a la información o dato personal.

De igual forma, el Hábeas Data también se podrá presentar contra quien es el custodio o responsable del manejo de la información que se recaba por parte de las empresas privadas que prestan o suministran servicios públicos con carácter exclusivo, en este caso con respecto a las que tiene que ver con los usuarios del servicio que suministran o prestan. Esto último tiene una gran relevancia, toda vez que amplía el marco de protección y supera así la tradicional concepción en cuanto a considerar como único infractor de los derechos fundamentales al Estado o a sus funcionarios en el ejercicio de sus funciones. Responde tal criterio, a lo que en otras legislaciones ha venido a responder la acción de amparo frente a actuaciones de particulares.

2.2.6 Del tribunal competente para conocer del Hábeas Data

En lo que a este aspecto se refiere, la ley 6 de 2002, dispone en su artículo 18 que:

"**Artículo 18**. La acción de Hábeas Data será de competencia de los Tribunales Superiores que conocen de la acción de Amparo de Garantías Constitucionales, cuando el funcionario titular o responsabilidad, registro o archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial. Cuando el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias o en toda la República, será de competencia del Pleno de la Corte Suprema de Justicia".

Como se sigue de la norma transcrita, el conocimiento de la acción de Hábeas Data se atribuye a las más altas esferas jurisdiccionales del Órgano Judicial, como lo vienen a ser los Tribunales Superiores de los Distritos Judiciales y la Corte Suprema de Justicia.

En cuanto a los Tribunales Superiores, el Hábeas Data será de competencia de los que conocen de la Acción de Amparo de los derechos constitucionales o fundamentales. En el caso de la máxima corporación de justicia del Órgano Judicial, será al Pleno de este alto tribunal, al cual corresponderá el dilucidar las causas que por razón de un Hábeas Data se promueve ante ésta, la Corte Suprema y ello cuando el titular o responsable del registro, archivo o banco de datos, a quien habiéndosele solicitado el acceso a alguno de los tipos de información o datos personales a los que se refiere la ley y no haya satisfecho adecuadamente tal requerimiento, tenga mando y jurisdicción en dos o más provincias o en el ámbito de toda la República.

2.2.7 En cuanto a la vía o formalidades para promoverla acción de Hábeas Data

Por la importancia que implica el tener acceso a los archivos, registros o bancos de datos, por el significado que para el sistema democrático tiene el conocimiento por parte de todos los que integran o componen la comunidad, el manejo de la administración pública en su carácter amplio o general, por

lo que para la persona humana representa el tener control de la información o dato que sobre ella se haya recabado, se parte del principio que para el ejercicio de la acción de Hábeas Data, no se requiera para su presentación de mayores formalidades. Se le da en cuanto a esto, un tratamiento similar al del Habeas Corpus.

Se establece en ese sentido en la primera parte del artículo 19 de la ley 6 de 2002, que la acción de Hábeas Data se promoverá "sin formalidades" y "sin necesidad de abogado", lo que viene a simplificar su formulación ante los tribunales competentes para conocer de ésta, en procura de lograr un acceso rápido y sin mayores obstáculos, a una tutela judicial efectiva en defensa de tan importantes derechos fundamentales, como lo son, el de derecho a la información y el de la intimidad, y dentro de éste, el de la protección de los datos personales. Por lo demás, esta concepción es cónsona con lo que en el artículo 212 de la Constitución se establece, al disponer que "las leyes procesales que se aprueben se inspirarán, entre otros principios", en el de la "ausencia de formalismos" y que "el objeto del proceso es el reconocimiento de los derechos consignados en la ley sustancial".

2.2.8 En cuanto al proceso al que da lugar la acción de Hábeas Data

En el citado artículo 19 de la ley en referencia, se deja consignado que "la acción de Hábeas Data se tramitará mediante procedimiento sumario... y en lo que respecta a la sustanciación, impedimentos, notificaciones y apelaciones, se aplicarán las normas que para estas materias se regulan en el ejercicio de la acción de Amparo de Garantías Constitucionales".

Significa lo anterior que serán aplicables las disposiciones que sobre cada uno de los aspectos a los que se aluden en el artículo 19 de la ley 6 de 2002, tiene previsto el Código Judicial para la acción de amparo, garantía constitucional que regulada en el artículo 50 de la Constitución, es

desarrollada en el Título III, del Libro IV del Código Judicial. Hay que entender que lo que tiene que ver con las normas que en materia de sustanciación, impedimentos, notificaciones y apelaciones que previstas con respecto al amparo han de aplicarse durante el trámite de la acción de Hábeas Data, habrán de hacerlo cónsono con la concepción propia de este nuevo mecanismo de protección del derecho a la información y de los datos personales que no es otra que la de brindar la mayor eficacia en la tutela de dichos derechos, particularidad de la que también está revestida, por lo demás, la acción de amparo.

2.3 La Proteccion de Datos Personales en Guatemala

A la fecha no existe en el ordenamiento guatemalteco una legislación específica para la Protección de Datos Personales ni el Habeas Data. Sin embargo, el Decreto 26-2008 Ley de Acceso a la Información Pública de Guatemala nos brinda ciertas definiciones y un procedimiento los cuales describiremos a continuación y siendo uno de los objetivos de ella garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que ella conste en archivos estatales, así como la actualización de los mismos, es lo más cercano la Protección de Datos en otros países donde este derecho se encuentra mejor desarrollado.

2.3.1 Definiciones

El artículo número 9 de la mencionada ley nos brinda las siguientes definiciones:

Datos Personales: Los relativos a cualquier información concerniente a personas naturales o identificables.

Datos Sensibles o Datos Personales Sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos

personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.

Habeas data: Es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de hábeas data o protección de datos personales de la presente ley.

2.3.2 Habeas Data en Guatemala

El Habeas Data se encuentra comprendido en el capítulo sexto de la Ley de Acceso a la Información Pública, pero antes de adentrarnos en el estudio de ello es importante definir quiénes son los sujetos involucrados de acuerdo a la misma ley:

Sujeto Activo: es toda persona individual o jurídica, pública o privada, que tiene derecho a solicitar, tener acceso y obtener la información pública que hubiere solicitado conforme a lo establecido en esta ley.

Sujetos Obligados: es toda persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución, y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del estado, o actos de la administración pública en general, que está obligado a proporcionar la información pública que se le solicite.

Con respecto al Habeas Data los sujetos obligados serán responsables de los datos personales y, en relación a estos deberán:

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos;
- Administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento;
- Procurar que los datos personales sean exactos y actualizados;
- Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

De ninguna manera los sujetos activos podrán utilizar la información obtenida para fines comerciales, salvo autorización expresa del titular de la información de igual manera los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones salvo que hubiere mediado previamente el consentimiento expreso del titular de los datos con la excepción de los motivos siguientes:

- Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

- Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
- Cuando exista una orden judicial;
- Los establecidos en esta ley;
- Los contenidos en los registros públicos;
- En los demás casos que establezcan las leyes.

Sin perjuicio de lo dispuesto en otras leyes, solo el titular de la información o su representante legal podrán solicitarla, previa identificación, que se les proporcione los datos personales que estén contenidos en sus archivos o sistemas de información. Los sujetos obligados deben entregar esta información dentro de los 10 días hábiles siguientes contados a partir de la presentación de la solicitud, el mismo plazo tendrá el obligado para notificar al solicitante la negativa de posesión de los datos solicitados.

Como el procedimiento descrito anteriormente, el titular de los datos o su representante legal podrán solicitar que se modifiquen sus datos personales contenidos en cualquier sistema de información, para este efecto el interesado deberá entregar una solicitud de modificaciones en la que señale las modificaciones a realizar y la documentación que soporte la petición, el sujeto obligado tendrá en este caso en un plazo no mayor a 30 días hábiles desde la presentación de la solicitud, entregar al solicitante una resolución donde se haga constar las modificaciones realizadas o bien, de manera fundamentada, informarle las razones por las cuales no procedieron las mismas.

Contra la negativa de entregar o corregir datos cabe el Recurso de Revisión.

2.3.3 Recurso de Revision

El recurso de revisión está contenido en el título cuarto de la ley de Acceso a la Información Pública y esta lo define como un medio de defensa jurídica que tiene por objeto garantizar que en los actos y resoluciones de los sujetos obligados se respeten las garantías de legalidad y seguridad jurídica, y establece a su vez como autoridad competente para conocer del recurso la máxima autoridad de la entidad contra la cual se dirige el recurso.

Se podrá hacer uso de este recurso dentro de los quince días siguientes a la notificación de la resolución que este causando perjuicios.

Lo podrá interponer el agraviado por sí mismo o por su representante legal, y será procedente el caso que al solicitante se le hubiere negado la información o alegue su inexistencia así como en los casos siguientes:

- El sujeto obligado no entregue al solicitante los datos personales solicitados, o lo haga en un formato incomprensible;
- El sujeto obligado se niegue a efectuar modificaciones, correcciones o supresiones a los datos personales;
- El solicitante considere que la información entregada es incompleta o no corresponda a la información requerida en la solicitud;
- En caso de falta de respuesta en los términos de la presente ley;
- Por vencimiento del plazo establecido para la entrega de la información solicitada;
- En los casos específicamente estipulados en esta ley.
- El solicitante deberá presentar la solicitud ante la máxima autoridad por escrito, debiendo contener lo siguiente:
- La dependencia o entidad ante la cual se presentó la solicitud;
- El nombre del recurrente y del tercero interesado si lo hay, así como el domicilio, lugar o medio que señale para recibir notificaciones;

- La fecha en que se le notificó o tuvo conocimiento del acto reclamado;
- El acto que se recurre y los puntos petitorios;
- Los demás elementos que considere procedentes someter a juicio de la máxima autoridad.

Una vez recibido el recurso la máxima autoridad resolverá dentro de los cinco días siguientes y la resolución que esta emita será de carácter público.

Dicha resolución podrá versar en dos sentidos ya sea confirmando la decisión de la unidad de información o bien revocando o modificando la decisión de la unidad de información y ordenar a la dependencia o entidad permitir el acceso al particular a la información solicitada, la entrega de la misma o las modificaciones, correcciones o supresiones a los datos personales sensibles solicitados.

Las resoluciones deben constar por escrito y establecer el plazo para su cumplimiento y los procedimientos para asegurar su ejecución.

Una vez emitida la resolución, exhortara en su caso al obligado para que dé pleno cumplimiento lo resuelto en un plazo de cinco días, bajo apercibimiento, en caso de incumplimiento, de certificar lo conducente ante el órgano jurisdiccional competente, sin perjuicio de dictare todas aquellas medidas de carácter administrativo y las que conduzcan a la inmediata ejecución de lo resuelto.

Una vez concluido todo el proceso anteriormente descrito se dará por terminada la fase administrativa, quedando a salvo el derecho del interesado de recurrir de ampara contra la resolución dictada.

2.4 La Protección de Datos Personales en Costa Rica

2.4.1 Generalidades

La protección de Datos en Costa Rica es un Derecho que a como en la mayoría de los países de la región es algo nuevo. La constitución costarricense en su artículo 24 establece el derecho a la intimidad, obligando así al Estado a crear mecanismos de defensa de este Derecho, es por esto que se crea el 26 de Junio del año 2011 la Ley 8968 Ley de Protección a la Persona Frente al Tratamiento de sus Datos Personales, que a continuación les describiremos a continuación de manera breve:

2.4.2 Objeto

Según la anteriormente mencionada ley el objeto de La Protección de Datos Personales es garantizar a cualquier persona el respeto a sus derechos, específicamente el derecho a la autodeterminación informativa en relación con su vida y su actividad privada.

2.4.3 Definiciones

Es importante antes que entremos en asuntos procedimentales que estudiemos ciertas definiciones que nos brinda la ley 8968 para tener así una mejor comprensión de todo:

Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

Datos personales: cualquier dato relativo a una persona física identificada o identificable.

Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (PRODHAB), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.

Interesado: persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.

Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.

Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales

y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

2.4.4 Principios

Entre todos los principios que estudiaremos a continuación tenemos como el más importante el de la autodeterminación informativa que consiste en regular el flujo de información que concierne a cada persona, derivado del derecho a la privacidad evitando que se propicien acciones discriminatorias. Aparte de este principio la ley 8968 nos hace referencia a los siguientes:

2.4.4.1 Principio de Consentimiento

Este principio tiene grandes secciones, la primera siendo el deber a informar que tiene la entidad interesada al titular de los datos acerca de la información de datos solicitados, la existencia de una base de datos así como la finalidad y el tratamiento que se le dará a estos. Dentro de este mismo principio tenemos también el otorgamiento de consentimiento que este deberá ser proporcionado por el titular de los datos o su representante legal y de manera escrita ya sea físico o electrónico, excepto en los casos en los que medie sentencia judicial, sean datos de lire acceso o bien que el titular por mandato de ley tenga la obligación de brindar dicha información.

2.4.4.2 Principio de Calidad de la Información

Solo se le deberá dar tratamiento a los datos que sean actuales, veraces, exactos y adecuados al fin para el que se desean tratar.

2.4.5 Tratamiento de los Datos

A los titulares de los datos les asisten distintos tipos de derechos frente al tratamiento de sus datos personales como es el derecho de acceso a la información que consiste en el derecho que posee el titular a ser informado acerca de la existencia de datos suyos, de que datos se tratan, con que finalidad se han recopilado y de qué manera se les ha dado o se les dará tratamiento.

También el titular posee el derecho a la rectificación de sus datos que consiste en el derecho que posee el titular a que sus datos sean rectificados, actualizados, cancelados o eliminados.

El derecho a la autodeterminación informativa se verá diezmado cuando se persiga:

a) La seguridad del Estado.
b) La seguridad y el ejercicio de la autoridad pública.
c) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.
d) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.
e) La adecuada prestación de servicios públicos.
f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

Existe una serie de categorías de datos especiales que requieren especial tratamiento:

- Datos Sensibles.

- Datos Personales de Acceso Restringido.
- Datos Personales de Acceso Irrestricto.
- Datos Referentes al Comportamiento Crediticio.

El responsable de la base de datos deberá adoptar todos los mecanismos necesarios tanto físicos como electrónicos para garantizar la seguridad y la confidencialidad de los datos almacenados en su base de datos. Bajo ningún punto se deberá almacenar información en bases de datos que no reúnan las condiciones mínimas de seguridad.

2.4.6 De la Agencia de Protección de Datos de los Habitante (PRODHAB)

La Ley 8968 en su artículo 15 manda a crear un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, denominado Agencia de Protección de Datos de los Habitantes.

La PRODHAB contara con las siguientes atribuciones:

- Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
- Llevar un registro de las bases de datos reguladas por esta ley.
- Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados.
- Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga

evidencia de un mal manejo generalizado de la base de datos o sistema de información.

- Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales.
- Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.
- Imponer las sanciones establecidas, en el artículo 28 de esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito.
- Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
- Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
- Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. En el ejercicio de sus atribuciones, la PRODHAB deberá emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

2.4.7 Procedimiento Realizado ante la PRODHAB

Cualquier persona que ostente un derecho subjetivo podrá denunciar ante la PRODHAB cualquier irregularidad o actuar no conforme a la ley de cualquier base de datos pública o privada.

Recibida la denuncia, se conferirá al responsable de la base de datos un plazo de tres días hábiles para que se pronuncie acerca de la veracidad de tales cargos. La persona denunciada deberá remitir los medios de prueba que respalden sus afirmaciones junto con un informe, que se considerará dado bajo juramento. La omisión de rendir el informe en el plazo estipulado hará que se tengan por ciertos los hechos acusados.

En cualquier momento, la PRODHAB podrá ordenar a la persona denunciada la presentación de la información necesaria. Asimismo, podrá efectuar inspecciones in situ en sus archivos o bases de datos.

Para salvaguardar los derechos de la persona interesada, puede dictar, mediante acto fundado, las medidas cautelares que aseguren el efectivo resultado del procedimiento. A más tardar un mes después de la presentación de la denuncia, la PRODHAB deberá dictar el acto final.

Contra su decisión cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

Si se determina que la información del interesado es falsa, incompleta, inexacta, o bien, que de acuerdo con las normas sobre protección de datos personales esta fue indebidamente recolectada, almacenada o difundida, deberá ordenarse su inmediata supresión, rectificación, adición o aclaración, o bien, impedimento respecto de su transferencia o difusión. Si la persona denunciada no cumple íntegramente lo ordenado, estará sujeta a las sanciones previstas en esta y otras leyes.

2.4.8 Procedimiento Sancionatorio

De oficio o a instancia de parte, la PRODHAB podrá iniciar un procedimiento tendiente a demostrar si una base de datos regulada por esta ley está siendo empleada de conformidad con sus principios; para ello,

deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

2.4.9 Sanciones y Faltas

Si se ha incurrido en alguna de las faltas tipificadas en esta ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes:

Para las faltas leves, una multa hasta de cinco salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.

Para las faltas graves, una multa de cinco a veinte salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.

Para las faltas gravísimas, una multa de quince a treinta salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República, y la suspensión para el funcionamiento del fichero de uno a seis meses.

2.4.9.1 Faltas Leves

a. Recolectar datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada, de conformidad con las especificaciones del artículo 5, apartado I.
b. Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

2.4.9.2 Faltas Graves

a. Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento informado y expreso del titular de los datos, con arreglo a las disposiciones de la ley.
b. Transferir datos personales a otras personas o empresas en contravención de las reglas establecidas en el capítulo III de la ley.
c. Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
d. Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a la ley.
e. Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

2.4.9.3 Faltas Gravísimas

a. Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 3 de la ley.
b. Obtener, de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.
c. Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la ley.
d. Proporcionar a un tercero información falsa o distinta contenida en un archivo de datos, con conocimiento de ello.
e. Realizar tratamiento de datos personales sin encontrarse debidamente inscrito ante la PRODHAB, en el caso de los responsables de bases de datos cubiertos por el artículo 21 de la ley.

f. Transferir a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares.

CAPITULO III: LA PROTECCION DE DATOS PERSONALES EN EL ORDENAMIENTO NICARAGUENSE

3.1 Definición

Según la ley 621, ley de Acceso a la Información Pública el Habeas Data es: La garantía de la tutela de datos personales privados asentados en archivos, registros, bancos de datos u otros medios técnicos, sean estos públicos o privados, cuya publicidad constituya una invasión a la privacidad personal

familiar, que tenga relevancia con respecto a datos sensibles de las persona, su vida íntima, incluyendo sus asuntos familiares, que se encuentre en poder de las entidades especificadas en al articulo1.

Se entiende por datos sensibles, los datos que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliaciones políticas, sindicales e información referente a la salud física y psicológica o a la vida íntima de las personas, en cualquier formato que se generen o almacenen.

De igual manera el Habeas Data garantiza el acceso de toda persona a la información que puede tener cualquier entidad pública sobre ella así como el derecho a saber por qué y con qué finalidad tienen esa información.

3.2 Naturaleza

La naturaleza del Habeas Data es de orden privado debido a que, basándonos en el artículo 26 de la Constitución Política de La Republica de Nicaragua de 1987 y en el concepto que nos brinda la ley 621 del 16 de mayo del 2007 publicada en La Gaceta, Diario Oficial número 118 del 22 de Junio del 2007, ley de Acceso a La Información Publica en su artículo 4 inciso b, este Derecho es subjetivo a cada persona debido a que su finalidad es garantizar la tutela de datos personales que puedan encontrarse contenidos en bases de datos de entidades públicas o privadas, siendo la persona titular de este derecho la única que puede otorgar el consentimiento para que sean tratados así como exigir la corrección, actualización o supresión de los mismos. Además, este derecho trata sobre la protección de la intimidad, el honor, la dignidad y la vida privada tanto personal como familiar y le brinda la facultad al titular de exigir saber cómo y porque se están tratando sus datos. Así mismo cabe resaltar que las legislaciones comparadas en el capítulo anterior,

establecen la naturaleza de este mecanismo de protección de datos personales de orden privado.

3.3 Objeto

Según la ley 787 del 21 de Marzo del 2012, publicada en La Gaceta Diario Oficial número 64 del 29 de Marzo del 2012, "ley de Protección de Datos Personales" en su artículo 1 nos dice que el objeto de la ley es " la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa." Esto nos dice que cualquier persona es protegida ante cualquier injerencia arbitraria de sus datos que se encuentren contenidos.

3.4 Sujetos

Los sujetos parte en el procedimiento de Habeas Data y en todo lo que respecta a la protección de datos personales son dos:

El Titular de la Información: Este puede ser una persona natural como cualquier individuo y una persona jurídica como una empresa, una sociedad anónima, una ONG, etc., es el dueño de la información que sobre él se esté dando tratamiento, a los derechos de este es a quien la ley de protección de datos personales da una especial tutela.

El Responsable de Los Ficheros de Datos: Los ficheros de datos para efectos de la legislación nicaragüense no son más que archivos, registros, bases o bancos de datos, públicos y privados, que contienen de manera organizada los datos personales, automatizados o no, siendo los responsables de estos cualquier ente público o privado, siendo estos cualquier institución gubernamental, en el ámbito público, y en el ámbito privado tenemos bancos, instituciones financieras, instituciones de educación, instituciones

comerciales y demás, que por la naturaleza de la actividad que realicen o les sea encomendada, necesiten en un momento dado tratar cierta información personal de terceros.

3.5 Legitimación Procesal

3.5.1 Legitimación Activa

El articulo 26 numerales 1 y 4 de nuestra constitución política reconoce el derecho que tiene toda persona a su vida privada y a la de su familia además de conocer la información que sobre ella hayan registrado las autoridades estatales así como el derecho de saber por qué y con qué finalidad tiene esa información.

Al hablar de persona, no solo se está refiriendo a la persona física sino también a la persona jurídica cuyos datos se encuentran archivados en los registros, pues si bien la constitución no hace tal aclaración, se encarga de ella el artículo 49 de la ley 787 Ley de Protección de Datos Personales, en donde aclara que cuando el recurso es promovido por una persona jurídica lo hará a través de sus representantes legales o apoderados legales que estas designen para tal efecto, dando así mayor seguridad a lo estipulado en el literal m del articulo tres en donde se establece quienes pueden ser titulares del derecho, así también lo consagra el reglamento de la ley 787 en su artículo 18 literal b dicho reglamento fue realizado mediante decreto número 36- 2012.

3.5.2 Legitimación pasiva

En lo que respecta a esta legitimación, el recurso de habeas data procede respecto de los responsables y usuarios de los ficheros de datos personales sean estos públicos o privados según lo estipula la ley 787 en su artículo 50.

3.6 Procedimiento

El Hábeas Data tutela, primordialmente, el derecho a la intimidad; esa zona más reservada y enigmática de toda persona o grupo, que en muchas ocasiones, a lo largo de la historia, fue invadida y castigada arbitrariamente. La intimidad constituye el talón de Aquiles de toda persona, punto que si se llega a atacar puede llevar a la destrucción personal y familiar.

Tradicionalmente, el almacenamiento de datos se realizaba de manera manual o a través de medios de fácil control. Hoy, con los constantes avances tecnológicos y el advenimiento del procesamiento electrónico de datos, su vigilancia y limitación se tornan más difíciles. Los datos se van adquiriendo, almacenando, transfiriendo o modificando de manera continua en fracción de segundos, e incluso ellos pueden llevar a traspasar las fronteras, sin que su titular tenga conocimiento de ello. Los datos, pueden llegar a crear el perfil de la persona, de manera tal que las entidades que las posean pueden alcanzar el íntegro conocimiento lo más secreto de una vida personal o familiar. Ellos evidencian aspectos o circunstancias personales que podrían ser gravemente amedrentados, pues los mismos no permanecen en secreto sino que, en la mayoría de los casos, son difundidos públicamente. Por otra parte, se debe tener en cuenta, que ésta actividad podría generar consecuencias indirectas, capaces de afectar otros ámbitos de la vida personal, como ser el patrimonial, social, etc.

Es por estos motivos antes expuestos que en nuestra legislación se reconoce este derecho y se le da un procedimiento distinto en vía administrativa como lo consagra el reglamento a la ley 787 el cual lo establece de la siguiente manera:

La tramitación de dicho recurso se inicia a instancia del titular del dato o representante legal dejando en claro el motivo de su reclamo y de los

preceptos que según el titular o su apoderado consideren violados según lo establece el reglamento en su artículo 38, en caso de que se haya señalado un tercero interesado en el proceso de la acción este se apersonara en el procedimiento mediante escrito en el que se acredite el interés jurídico que este tiene en dicha acción, esto lo tendrá que hacer antes del cierre de instrucción, para tal caso deberá de adjuntar en su escrito el documento que lo acredite y de certeza de su personalidad esto cuando no actúe en nombre propio además que deberá adjuntar las pruebas documentales que tenga a su bien para ofrecerlas en el proceso. Dicha acción de reclamo deberá ser interpuesta ante la dirección de protección de datos personales (DIPRODAP), la cual dará traslado a la misma al responsable del fichero de datos anexándole copias de todos los documentos presentados por el recurrente para que este en el término de quince días exprese lo que tiene a bien ante dicha acción. Después de presentadas las pruebas por parte del responsable del fichero la DIPRODAP podrá pedir al responsable del fichero las pruebas que estime pertinentes para dar la solución al conflicto originado para que una vez concluido el análisis de pruebas la DIPRODAP notificara al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días hábiles siguientes a su notificación.

Es importante resaltar que la DIPRODAP tiene que aceptar o rechazar la solicitud de la acción en un plazo no mayor de diez días hábiles a partir de su recepción, una vez admitida será notificada la admisión al solicitante y se le correrá traslado al responsable del fichero en un plazo no mayor de diez días hábiles.

Dentro de todo este proceso en vía administrativa no puede faltar el tramite conciliatorio el cual se lleva a cabo una vez que la DIPRODAP notifique a las partes para que comparezcan a realizar dicho trámite, este se llevara a

cabo una vez admitida la solicitud de protección de datos por el titular, el procedimiento que regirá este trámite es el que estime a bien la DIPRODAP mediante una normativa de carácter general.

Los acuerdos a los que se llegaren en el proceso conciliatorio tienen carácter vinculante para las partes lo cual se hará constar por escrito para que la solicitud de protección de los datos hecha por el titular quede sin efectos, y para el cumplimiento de dichos acuerdos la DIPRODAP será el ente fiscalizador para el cumplimiento de estos.

Una vez cumplido todo el trámite de iniciación del proceso en vía administrativa la DIPRODAP tendrá un plazo de cincuenta días hábiles, contados a partir de la fecha de presentación de la solicitud de acción correspondiente, cuando haya causa justificada la DIPRODAP podrá ampliar por una vez y hasta por un periodo igual este plazo. Siempre y cuando las solicitudes de la acción cumplan con los requisitos establecidos en el artículo 43 del presente reglamento.

De no cumplir con los requisitos o a falta de uno de estos y la DIPRODAP no cuente con los elementos necesarios para subsanarlos se prevendrá al titular de los datos para que este los subsane por una sola vez y dentro de un plazo de cinco días hábiles a partir de la notificación, a falta de la subsanación del error presentado en la solicitud de la acción de protección de los datos esta se tendrá por no presentada, pero una vez que este error sea notificado y subsanado la notificación o prevención tiene el efecto de interrumpir el plazo que tiene la DIPRODAP para resolver la solicitud de protección de datos.

Una vez realizado todo el proceso de iniciación del trámite administrativo la DIPRODAP emitirá su resolución una vez que se tenga por evacuadas todas las pruebas, y se pondrán a disposición de las partes para que estos en caso

de inconformidad formulen nuevos alegatos en un plazo de cinco días hábiles contados a partir de la notificación de la resolución, una vez transcurrido dicho plazo se dará por culminado dicho trámite y la DIPRODAP emitirá su resolución de manera definitiva.

Como en todo recurso este no es la excepción de las causales de denegación de la solicitud siendo causas de denegación de la solicitud del recurso las siguientes según lo establecido en el artículo 39 del reglamento a la ley 787:

Cuando la DIPRODAP no sea competente.

Cuando la DIPRODAP haya conocido anteriormente de la solicitud de acción de protección de datos personales contra el mismo acto y haya resuelto de manera definitiva respecto del mismo recurrente.

Cuando se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular de los datos que pueda tener por efecto modificar o revocar el acto respectivo.

3.7 Procedimientos de inspección de ficheros

Los procedimientos de inspección a los ficheros de datos es una de las facultades que la ley le confiere a la dirección de protección de los datos personales (DIPRODAP),dichos procedimientos se les efectúan a los ficheros de datos por medio de visitas de verificación y control sean estos públicos o privados, dichas visitas la realizan inspectores de la DIPRODAP los cuales son personas debidamente capacitadas por la DIPRODAP para ejercer ese cargo y realizar las revisiones pertinentes en el fichero de acuerdo al programa de visitas y que se encuentren operando en el almacenamiento de datos dentro del territorio nacional , dichas visitas se efectúan con el objetivo de fijar el grado de responsabilidad y cumplimiento de las normas regulatorias de la materia o bien aportar mayores argumentos jurídicos que

apoyen una causa abierta ante la DIPRODAP los cuales les servirán a esta para dictar una resolución definitiva ante tal situación. Tal visita tiene un tiempo de duración de un día este podrá prorrogarse cuando la visita se tenga que hacer en más de un lugar en donde se levantaran actas parciales que se agregaran en su total al momento de la culminación de la inspección.

Para llevar a cabo tal procedimiento se necesitan cumplir con ciertos requisitos y procedimientos establecidos en la ley 787 y su reglamento los cuales son los siguientes:

Para que las personas capacitadas como inspectores de ficheros deberá portar el documento emitido por la dirección de protección de datos personales que lo acredite como tal así como también cumplir con los requisitos establecidos en el artículo 51 del reglamento de la ley en donde se establece los requisitos de identificación de los inspectores para que estos puedan ejercer el proceso de inspección además que tiene que llevar la orden de inspección firmada por la autoridad competente en la que deberán de estar los requisitos de ley establecidos en el artículo 43 del reglamento.

Este procedimiento de inspección se realiza en los ficheros de datos sean estos públicos o privados con el objeto de velar que se cumplan con las garantías legales establecidas en la ley de la materia, estos procedimientos se podrán realizar a petición de parte interesada o bien la DIPRODAP podrá actuar de oficio en donde se le requerirá al responsable del fichero de datos la documentación necesaria o bien realizando las visitas correspondientes a los centros o establecimientos en donde se sitúen los ficheros. Cuando la inspección se vaya a realizar por denuncia de parte interesada la DIPRODAP señalara el recibido de la misma y podrá solicitarle al denunciante la documentación necesaria para fijar o no la procedencia de la denuncia.

En dicho proceso de inspección al momento de la culminación del mismo el inspector deberá de levantar un acta de inspección de la cual se le entregara una copia al inspeccionado, en dicha acta deberá de constar por lo menos la indicación del lugar, la fecha y la hora en que se realiza la inspección, los datos generales de la persona con quien se coordinó la inspección del fichero este puede ser el responsable, administrador, etc. o similares de la compañía en donde se realizó la inspección, se realizara una breve referencia de la orden de inspección en caso de denuncia expedida por la autoridad competente y la motivación de la misma, por ultimo deberá contener el detalle de los hallazgos de las accione u omisiones por parte del responsable del fichero que estén en pleno cumplimiento de las normas y demás disposiciones regulatorias de la actividad o bien que constituyan o presuman infracciones y faltas flagrantes o simuladas a las mismas, haciendo una descripción detallada y con la mayor precisión posible. Además de presentar los requisitos establecidos en el reglamento a la ley de protección de datos personales:

Contenido de las Actas de Inspección. En las actas de inspección se hará constar lo siguiente:

a) Nombre, denominación o razón social del responsable del fichero de datos;
b) Hora, día, mes y año en que se inicie y concluya la inspección;
c) La dirección de las oficinas del responsable del fichero de datos donde se practique la inspección, así como, número telefónico, fax, correo electrónico u otra forma de comunicación disponible;
d) Número y fecha de la orden que la motivó;
e) Nombre y cargo de la persona con quien se entendió la inspección;
f) Nombre y domicilio de las personas que fungieron como testigos;
g) Datos relativos a la actuación;

h) Declaración del responsable del fichero de datos o encargado, si quisiera hacerla, y
i) Nombre y firma de quienes intervinieron en la inspección, incluyendo los de quienes la hubieran llevado a cabo. Si se negara a firmar el inspeccionado, su representante legal o la persona con quien se entendió la inspección, ello no afectará la validez del acta, debiendo el personal inspector asentar la razón relativa.

Los responsables de ficheros de datos a quienes se haya levantado acta de inspección, podrán formular observaciones en el acto de la inspección y manifestar lo que a su derecho convenga en relación a los hechos contenidos en ella, o bien, por escrito dentro del término de los cinco (5) días hábiles siguientes a la fecha en que se hubiere levantado.

3.8 Infracciones, Sanciones y su Procedimiento

Una vez que se haya llevado todo el procedimiento administrativo correspondiente y mediante las pruebas aportadas por las partes se llegue a confirmar la violación a la norma reguladora de los datos personales, esta establece un proceso de responsabilidades administrativas las cuales pueden ser infracciones leves o graves según el caso, las cuales conllevan un proceso de sanciones estipulado en el reglamento a la ley 787.

Se pueden considerar como faltas leves según lo estipulado en la ley de protección de datos personales: el tratar los datos sin el consentimiento del titular de los datos ya que para esto se necesita dicho acto para poder ser tratados, omitiera la inclusión, complementación, rectificación etc. de los datos personales que se encuentren en los ficheros sean estos públicos o privados sea este acto que se haga de oficio o a petición del titular, el incumplimiento de las instrucciones hechas o emitidas por la DIPRODAP entre otras.

Así también hay otras acciones que se pueden cometer por parte de los responsables de los ficheros las cuales son consideradas por los legisladores como faltas graves tal es el caso de que se haga el tratamiento de datos por medios fraudulentos o que se realice dicho acto en contraposición con lo establecido con la norma regulatoria, impedir u obstaculizar el ejercicio del derecho a la autodeterminación informativa que le otorga en el artículo 26 numerales 1 y 4 de la norma constitucional al titular del dato así como el negarle el derecho a acceder a la información solicitada, violentar el secreto profesional que debe ser guardado por disposición legal, no mantener las condiciones mínimas para el aseguramiento de los datos contenidos en los ficheros en el cual tiene que existir confidencialidad e integridad para la protección de dichos datos así como también se considera falta grave la obstrucción a las inspecciones que realice la DIPRODAP y reincidir en las infracciones leves.

Después de que la violación a la norma sea confirmada por la DIPRODAP esta tendrá que aplicar sanciones sin perjuicio de las responsabilidades administrativas de los responsables o usuarios de los ficheros de datos públicos, de lo cual pueden derivar responsabilidades por daños y perjuicios los cuales se derivan de las infracciones a la ley así como también en las sanciones penales contempladas en la legislación penal en el apartado de los delitos contra la vida privada y la inviolabilidad del domicilio, capítulo 1, pero a la DIPRODAP solo le compete aplicar las sanciones administrativas las cuales pueden caer en la suspensión de operaciones relacionadas con el tratamiento de los datos personales, el apercibimiento y hasta la clausura o cancelación de los ficheros de datos personales de manera temporal o definitiva. Cabe señalar que en caso de la conducta sea considerada como una falta leve se le aplicara al infractor dependiendo del caso y el daño que esta pueda originar la sanción acarreara el apercibimiento o la suspensión

de operaciones según sea el caso, y al momento de que la infracción sea considerada como una falta grave al infractor según sea el caso la clausura o cancelación del fichero infractor.

Para llevar a cabo la aplicación de las sanciones por la comisión de faltas sean estas leves o graves según el caso se tendrá que seguir el procedimiento establecido en el reglamento de la ley de protección de datos en su capítulo VIII.

Dicho procedimiento se iniciara con la notificación al presunto infractor y cuando la DIPRODAP determine las presuntas infracciones cometidas a la ley y a las regulaciones que de ella se deriven y sean realizadas por el responsable del fichero dichas infracciones deberán ser susceptibles de sanción conforme a la norma.

La notificación hecha por la DIPRODAP tendrá que ir acompañada de un informe que describa los hechos que describan los hechos de la presunta infracción, corriéndole traslado al responsable del fichero infractor para que presente las pruebas que tenga a bien en un plazo de 15 días hábiles después de notificado, este al momento de su contestación a la acción deberá manifestarse concretamente referente a los hechos que se le amputan de manera que los afirme o lo niegue de manera que los narre o señale como ocurrieron así como también presentando las pruebas pertinentes, estas pruebas pueden ser testimonial, documental o pericial según sea el caso, en caso de que las pruebas ofrecidas sean testimonial o pericial se precisarán los hechos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. A falta de estos señalamientos se tendrán por no ofrecidas dichas pruebas.

Ya presentada las pruebas pertinentes por las partes la DIPRODAP las podrá aceptar o rechazar para proceder a su evacuación, de ser necesario la DIPRODAP mandara a notificar a las partes para que asistan a una audiencia de evacuación de las pruebas que así lo requieran, en dicha audiencia se levantara un acta que contendrá la audiencia así como también la evacuación de las pruebas.

Ya evacuadas las pruebas se le notificara al infractor que cuenta con un plazo de cinco días hábiles a partir de la notificación para que presente alegatos que tenga a bien. Ya por transcurrido el plazo para que esté presente sus alegatos se tendrá por cerrado el proceso de instrucción y la DIPRODAP contara con un plazo de cincuenta días hábiles siguientes a los que inicio el procedimiento para emitir su resolución en caso de que haya causa justificada esta podrá prorrogar el plazo por un plazo igual y no mayor al estipulado, de existir inconformidad por las partes con la resolución emitida por la DIPRODAP se podrán emplear los recursos establecidos en la ley en su artículo 52 párrafo segundo.

3.9 Recurso de Habeas Data

Este recurso se ha creado para proteger los derechos de los nicaragüenses a su vida privada y autodeterminación así como también al respeto de su honra y conocer en todo momento la información que sobre ellos se maneje, estos derechos se encuentran consagrados en nuestra Constitución Política en el artículo 26 numerales 1, 3 y 4.

Antes de la institucionalización de este recurso, la ley 787, ley de Protección de Datos Personales indicaba en su artículo 52 que una vez agotada la vía administrativa el titular de los datos podía recurrir de amparo ante la Corte Suprema de Justicia, en contra de la resolución dictada por la DIPRODAP. En fecha del 30 de Enero del 2013 se aprobó la ley 831 Ley de Adición y

Reformas a la Ley Numero 49, ley de Amparo, la cual creaba el recurso de Habeas Data y lo incorporaba en esta Ley Constitucional, quedando así formalmente establecido un proceso jurisdiccional para la protección de datos personales.

El recurso de Habeas Data se encuentra comprendido en los artículos 87 al 97 de la ley de Amparo, en estos artículos se describe el procedimiento el cual exponemos a continuación:

3.9.1 Motivación del Recurso

Este recurso puede ser solicitado por cualquier persona por tres motivos esencialmente:

- Acceder a información personal que se encuentre en bases de datos de terceros, sean estas públicas o privadas, y de esta se estén generando algún tipo de investigación, dictámenes, estudios, etc.
- Para exigir la oposición, bloqueo, modificación, rectificación, actualización o cancelación de datos personales sensibles ya sean físicos o electrónicos almacenados en ficheros de datos propiedad de entidades públicas o privadas.
- Para exigir la oposición, bloqueo, modificación, rectificación, actualización o cancelación de datos personales sensibles que vulneren derechos y garantías constitucionales.

3.9.2 Interposición del Recurso y Tribunal Competente

El recurso de Habeas Data podrá ser interpuesto por:

- Persona natural afectada.
- Tutor, sucesor o apoderado de la persona natural afectada.
- Persona jurídica afectada por medio de su representante legal.

Para la interposición de este recurso la persona legitimada deberá haber agotado el procedimiento administrativo descrito con anterioridad en este mismo capítulo y tendrá un plazo de 30 días después de notificada la resolución de la autoridad administrativa competente en materia de protección de datos personales.

Este recurso se dirige en contra de los responsables de ficheros de datos o cualquier otra persona que hubiere hecho un uso indebido de la información contenida en los ficheros ya sean estos públicos o privados

El responsable de los ficheros no podrán alegar confidencialidad de la información que se les requiera, solo será así en el caso que se afecten o comprometan fuentes de información periodística. Cuando este sea el caso la Sala Constitucional de la Corte Suprema de Justicia como órgano competente de conocer este recurso, en los casos que la ley justifique la confidencialidad, tomara conocimiento personal de la información garantizando su confidencialidad.

El escrito del Recurso deberá contener los siguientes requisitos:

- Contra quien va o se presume que va el Recurso, su domicilio, calidad y demás elementos identificativos de las partes.
- La descripción de en qué consiste la vulneración de derechos, las circunstancias, pruebas y elementos con que cuente el afectado acerca de la lesión sufrida.
- Copia de la resolución que agota la vía administrativa.

Se podrá solicitar en este escrito la suspensión de los actos que están produciendo la vulneración de los actos, ante esto la Sala de lo Constitucional debe pronunciarse de inmediato. Esta medida puede ser oficiosa o a petición de parte.

De faltar alguno de los requisitos señalados anteriormente se notificara al recurrente quien tendrá un plazo de 3 días para subsanar errores, de no hacerlo o de persistir los errores el Recurso se tendrá por no interpuesto.

Si el escrito reúne todos los requisitos, se notificara al responsable del fichero quien tendrá un plazo de tres días para pronunciarse al respecto de la causa y podrá a su vez en el escrito de contestación aportar las pruebas que estime conveniente. Ante la negativa de contestación se tendrán por ciertos todos los criterios expresados por el recurrente.

Si por medio del examen de la causa la Sala Constitucional determina que existe una lesión al derecho del recurrente, esta dictara las medidas necesarias para el cumplimiento de la sentencia. La misma sala deberá velar que no se divulgue información cuyo titular podría resultar afectado por su difusión.

Una vez admitido el recurso, se le ordenara al recurrido exhibir la información solicitada por el recurrente. Cuando se trate de información confidencial, la Sala procederá de la manera ya descrita y delimitara los datos a los que el recurrente podrá tener acceso.

La suspensión de los actos que están vulnerando derechos procederá de manera precautelar en los casos que:

a) Cuando el dato se esté transmitiendo y así eliminando su confidencialidad.
b) Cuando los datos sensibles que se estén tratando revelen ideología, religión, raza, orientación sexual, filiación política, entre otros, se debe suspender hasta determinar si hubo o no consentimiento del recurrente.
c) Cando la información sea inexacta, falsa o desactualizada.

d) Cuando la difusión de la información, vaya a causar daños irreparables en el futuro.

La Corte dictara la suspensión de los actos tomando en cuenta la urgencia del asunto para evitar futuros daños. Esto también afectara a registros conexos donde se puedan encontrar los datos objeto del recurso.

3.9.3 Sentencia y sus Efectos

La Sala Constitucional de la Corte Suprema de Justicia dictara sentencia dentro de los 30 días siguientes a la admisión del Recurso. De ser declarado a lugar en Recurso se ordenara restituir el pleno goce del derecho constitucional vulnerado y además ordenara la supresión y eliminación de la información o datos impugnados en los casos que:

- Cuando la información haya sido obtenida para transmitirla a terceros no legitimados para obtenerla.
- Cuando haya tratamiento de datos sensibles y no exista consentimiento expreso del titular para ello.
- Cuando la permanencia de los datos en el fichero ya haya perdido utilidad alguna, por haber prescrito o por haber cumplido su finalidad.
- Cuando la información o los datos hayan sido obtenidos de manera ilegal o ilegitima.
- Cuando la información no sea necesaria para los fines del fichero.

La Sala de lo Constitucional ordenara al responsable del o los ficheros la supresión, modificación, alteración o corrección correspondiente. Así mismo le dará el derecho demandar el pago de costas, daños y perjuicios ocasionados por el responsable de ficheros.

CONCLUSIONES

A través de la realización de nuestro trabajo investigativo hemos llegado a las siguientes conclusiones:

1. La Protección de Datos Personales ha tenido en los últimos tres cuartos de siglo una aceleración en su evolución a nivel internacional.
2. La gran mayoría de las constituciones de Latinoamérica consagran el derecho a la autodeterminación informativa y a la vida privada de los individuos.
3. Algunos países aún se encuentran atrasados en materia de protección de datos, no cuentan con mecanismos concretos o estos son disfuncionales.

4. Nicaragua cuenta con una legislación amplia y completa, en la cual se establecen mecanismos administrativos y jurisdiccionales para la protección de datos pero, a pesar de la modernidad y amplitud de las leyes, estas carecen de eficacia material al no ser implementadas tras años de su aprobación, esto lo pudimos constatar mediante visitas a la Oficina de Acceso a la Información Publica del Ministerio de Hacienda y Crédito Público que sería el ente al cual la DIPRODAP estaría adscrita encontrándonos con que dicha Dirección no ha sido creada aun, así como también realizamos la consulta a la Sala Constitucional de la Corte Suprema de Justicia acerca de casos de Habeas Data tramitados, encontrándonos con que no se ha tramitado Recurso alguno.
5. La población en general no está muy familiarizada con este derecho que si bien es novedoso no deja de ser de vital importancia defenderlo sobre todo en nuestro mundo actual.
6. Existen organizaciones internacionales que se mantiene vigilante a la evolución e implantación de la protección de datos personales y a su vez la impulsan.
7. La protección de Datos Personales y el Habeas Data son de vital importancia ya que debido al avance de la tecnología y las telecomunicaciones, nuestros datos y nuestra privacidad cada día se encuentran más vulnerables a robo y mal manejo por lo cual cada día se requieren mejores sistemas de protección.

RECOMENDACIONES

A partir de las conclusiones alcanzadas podemos realizar las siguientes recomendaciones:

- Mayor observancia y promoción internacional a la correcta y eficaz implementación de mecanismos de Protección de Datos Personales por parte de Organismo Internaciones.
- En el caso concreto de Nicaragua la creación de la DIPRODAP ya que tres años tras ser aprobada la ley que manda su creación esta no lo ha sido motivo por el cual no se han puesto en marcha ninguno de los mecanismos de protección ni administrativos ni jurisdiccionales.

- Impulsar campañas de promoción a la ley para que la población en general tenga mayor conocimiento de los derechos que les asisten ante el tratamiento de su información por parte de terceros.

BIBLIOGRAFIA

Fuentes del Conocimiento

- Constitución Política de la Republica de Nicaragua.
- Constitución Política de la Republica de Colombia.
- Constitución Política de la Republica de Panamá.
- Constitución Política de la Republica de Guatemala.
- Constitución Política de la Republica de Costa Rica.
- Decreto Nº 57-2008 Ley de Acceso a la Información Pública de Guatemala.
- Ley Estatutaria 1581 del 17 de Octubre del 2012 de Colombia.

- Decreto Nº 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica.
- Ley 787 del 21 de Marzo del 2012, Ley de Protección de Datos Personales de Nicaragua.
- Ley Nº 621 del 16 de Mayo del 2007, Ley de Acceso a la Información Publica de Nicaragua.
- Ley Nº 49, Ley de Amparo de Nicaragua.
- Ley Nº 6 del 22 de Febrero del 2002, Que Dicta Normas Para la Transparencia en la Gestión Publica, establece la Acción de Habeas Data y otras Disposiciones.

Documentos Digitales

- www.iij.ucr.ac.cr/arhivos/publicaciones/revista
- www.informatica-juridica.com/trabajos/lavisioncosntitucionaldelhabeasdata
- http://www.redipd.org/noticias_todas/2013/tribuna/common/Mapalatinoamericanopdp1985201322032013NRemolina.pdf
- www.habeasdatacolombia.uniandes.edu.com/wp-content/uploads/1-Antonio-Martino-Final.pdf
- http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Antonio-troncoso_FINAL.pdf
- http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/3_Alfredo-Chirino_FINAL.pdf
- http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_Nelson-Remolina_FINAL.pdf
- www.slidesshare.net/smith19/proceso-de-habeas-data
- www.cechoc.cl/htm/revista/docs/const/2n_3_2005/4.pdf

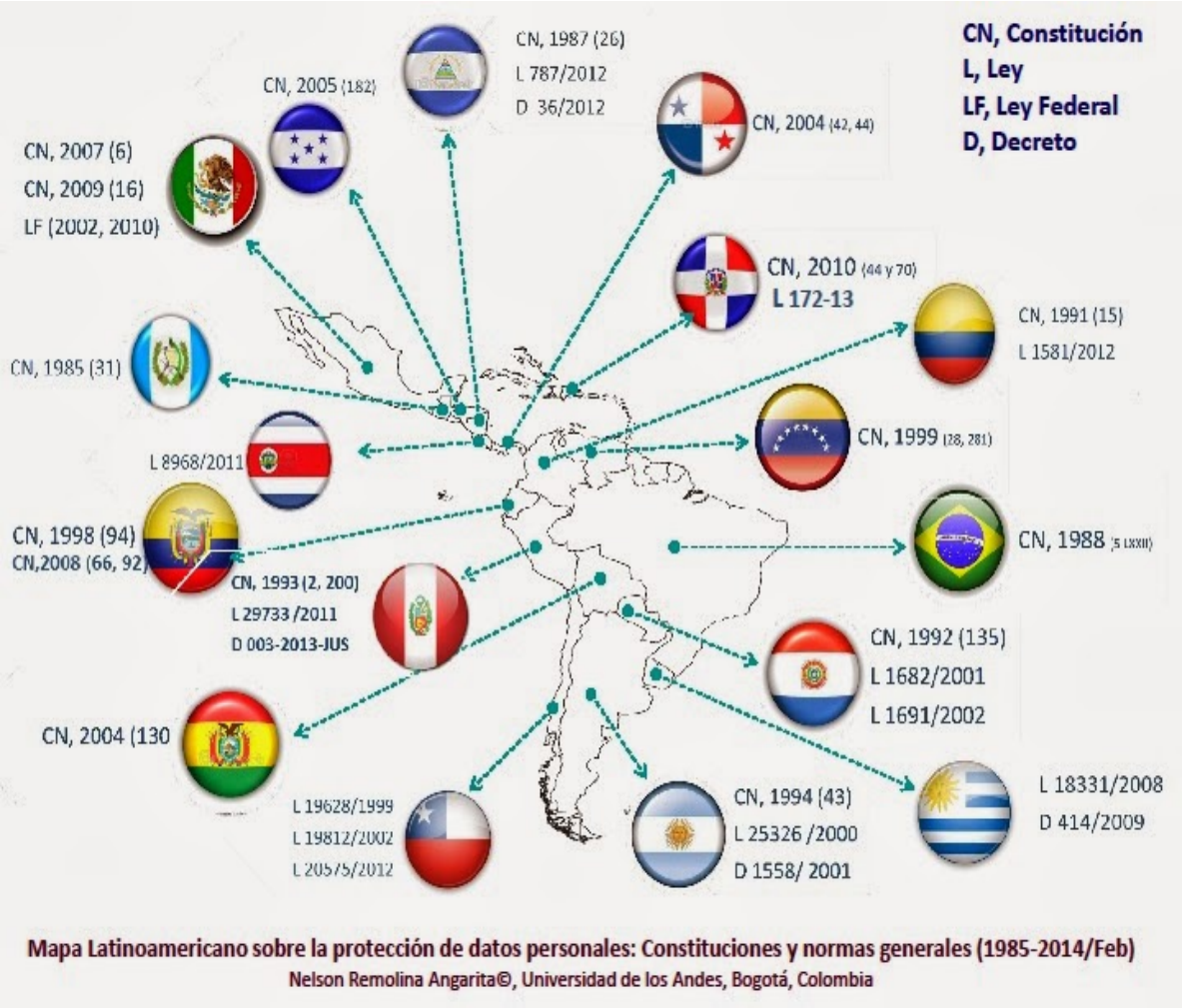
- www.inej.edu.ni

Obras Consultadas

- ESCOBAR FORNOS, Iván, Derecho Procesal Constitucional "La Constitución y su Defensa", Hispamer, Managua, 1999.
- ESCOBAR FORNOS, Iván, Introducción al Derecho Procesal Constitucional, Editorial Porrúa, México D.F., 2005.
- FLORES DAPKEVICIUS, Rubén, Amparo, Habeas Corpus y Habeas Data, Editorial BDF, Montevideo-Buenos Aires, 2011.

ANEXOS

Mapa Latinoamericano Sobre la Protección de Datos


CN, Constitución
L, Ley
LF, Ley Federal
D, Decreto
CN, 1987 (26)
L 787/2012
D 36/2012
CN, 2005 (182)
CN, 2004 (42, 44)
CN, 2007 (6)
CN, 2009 (16)
LF (2002, 2010)
CN, 2010 (44 y 70)
L 172-13
CN, 1991 (15)
L 1581/2012
CN, 1985 (31)
L 8968/2011
CN, 1999 (28, 281)
CN, 1998 (94)
CN,2008 (66, 92)
CN, 1988 (5 LXXII)
CN, 1993 (2, 200)
L 29733 /2011
D 003-2013-JUS
CN, 1992 (135)
L 1682/2001
L 1691/2002
CN, 2004 (130
L 19628/1999
L 19812/2002
L 20575/2012
CN, 1994 (43)
L 25326 /2000
D 1558/ 2001
L 18331/2008
D 414/2009
Mapa Latinoamericano sobre la protección de datos personales: Constituciones y normas generales (1985-2014/Feb)
Nelson Remolina Angarita©, Universidad de los Andes, Bogotá, Colombia