



# Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data de Honduras

Dr. Lester Ramírez Irías  
Consultor Investigador  
Enero 2014

## ÍNDICE

NOTA INTRODUCTORIA .....	2
CONTENIDO .....	5
TÍTULO I DISPOSICIONES GENERALES.....	5
CAPÍTULO ÚNICO .....	5
TÍTULO II PRINCIPIOS Y DERECHOS BÁSICOS PARA LA PROTECCIÓN DE DATOS PERSONALES ...	7
CAPÍTULO I PRINCIPIOS RECTORES.....	7
CAPÍTULO II DERECHOS DEL TITULAR DE LOS DATOS .....	9
TÍTULO III PROCEDIMIENTOS PARA HACER EFECTIVOS LOS DERECHOS .....	12
CAPÍTULO ÚNICO .....	12
TÍTULO IV DEBERES DE LOS RESPONSABLES .....	14
CAPÍTULO ÚNICO .....	14
TÍTULO V SEGURIDAD DE DATOS .....	16
CAPÍTULO ÚNICO .....	16
TÍTULO VI CATEGORIAS ESPECIALES DE DATOS .....	17
CAPÍTULO ÚNICO .....	17
TÍTULO VII TRANSFERENCIA DE DATOS .....	19
CAPÍTULO ÚNICO .....	19
TÍTULO VIII DISPOSICIONES SECTORIALES .....	22
CAPÍTULO I BASES DE DATO DE TITULARIDAD PÚBLICA .....	22
CAPÍTULO II BASES DE DATO DE TITULARIDAD PRIVADA.....	23
TÍTULO IX DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN .....	24
CAPÍTULO I DEL INSTITUTO DE ACCESO A LA INFORMACION PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.....	24
CAPÍTULO II DEL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS .....	27
CAPÍTULO III DEL PROCEDIMIENTO DE VERIFICACIÓN.....	29
CAPÍTULO III DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES.....	30
CAPÍTULO III DE LAS INFRACCIONES Y SANCIONES.....	30
TÍTULO X DE LA ACCIÓN DE HÁBEAS DATA.....	32
TÍTULO XI CÁNONES.....	34
TRANSITORIOS .....	35

## **NOTA INTRODUCTORIA**

Este anteproyecto es el resultado de la revisión de los estándares internacionales en materia de protección de datos personales, específicamente los trabajos que viene realizando la Organización de las Naciones Unidas, a través de la *Resolución 45/95 Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales*; el derecho comunitario europeo, mediante la *Directiva 95/46/CE* relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y, la labor del foro regional para el intercambio de experiencias que realiza la Red Iberoamericana de Protección de Datos, reflejada en la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal*.

Complementado la doctrina jurídica y la revisión de los estándares internacionales, toma en cuenta el análisis comparativo de cinco legislaciones referenciales que han de contribuir a sentar las bases para una ley de protección de datos personales y acción de hábeas data en Honduras:

1. Ley General de Protección de Datos Personales de Colombia.
2. Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica.
3. Ley Orgánica de Protección de Datos de España.
4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México.
5. Ley de Protección de Datos Personales y Acción de Habeas Data de Uruguay.

Este Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data de Honduras es un primer esfuerzo de proponer una legislación que mejor se pueda adaptar al contexto institucional, jurídico, social y económico de Honduras. A continuación se presenta una breve explicación de su estructura y contenido.

- I. El Título I “Disposiciones Generales”, establece el objeto de la Ley, el cual consiste en la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. También detalla el ámbito de aplicación de la Ley, haciendo la salvedad que no será aplicable a las bases de datos de personas naturales destinadas a actividades personales o domésticas; las que tienen por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito; las creadas y reguladas por normas especiales, como las del sector financiero; y, aquellas que contengan información periodística y otros contenidos editoriales. Finalmente, el Título I, define una serie de términos jurídicos y técnicos en materia de protección de datos.
- II. El Título II “Principios y Derechos Básicos para la Protección de Datos Personales”, presenta la base de la interpretación y aplicación de la normativa de protección de datos.

Ha de ser la brújula que guía el actuar de los titulares y responsables, garantiza la efectiva aplicación del derecho a los titulares y orientan las decisiones del órgano de control como las instancias judiciales. La recopilación de los principios parte de la Resolución 45/95 de la ONU, los establecidos en las legislaciones costarricense, española, mexicana, uruguaya y costarricense, contextualizado a terminología legal hondureña.

- III. El Título III “Procedimientos para hacer efectivos los Derechos”, describe los procedimientos para ejercer los Derechos de Acceso, Rectificación, Eliminación y Oposición -Derechos AREO- ante el Responsable del Tratamiento. Para la recolección de datos, la persona titular o su representante, debe manifestar su consentimiento por escrito; ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. Se incluye el formato y la información que debe contener la solicitud que presenta el Titular de los Datos Personales, los plazos que ha de resolver el Responsable del Tratamiento y atiende posibles casos especiales que se pueden dar en la práctica o situaciones imprevistas.
- IV. El Título IV “Deberes de los Responsables” enlista los principales deberes que ha de tener el Responsable del Tratamiento y el Encargado del Tratamiento. Es importante aclarar que ambos sujetos son considerados obligados pero no solidarios. El Responsable del Tratamiento por ser el que obtiene el consentimiento del Titular, es a quien recae el grueso de las obligaciones y sanciones por incumplimiento. Por otro lado, el Responsable del Tratamiento debe asegurar que los datos que brinde al Encargado son correctos y cerciorarse del manejo adecuado de estos por parte de éste.
- V. El Título V “Seguridad de datos”, establece los lineamientos para el Responsable del Tratamiento y el Instituto de Acceso a la Información Pública (IAIP) en materia de seguridad. El responsable de la base de datos tiene la obligación de adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de la información, evitando su alteración, destrucción o acceso no autorizado. Consecuentemente, quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aún después de finalizada su relación con la base de datos. Mientras que al IAIP, como órgano regulador establecerá los requisitos y las condiciones que deban reunir las bases de datos, y de las personas que intervengan en la recolección, almacenamiento y uso de los datos..
- VI. El Título VI “Categoría Especiales de Datos”, norma el tratamiento de los datos sensibles que utilizados de manera discrecional o abusiva pueden infringir la privacidad e imagen de la persona, causando daños patrimoniales, discriminación. Asimismo se regula los datos que manejan los operadores de telecomunicaciones, aquellos que se utilizan para fines publicitarios y los buros de crédito. En este último caso, a pesar que la CNBS tiene su propia normativa, se recalca que los derechos AREO se aplican también a normas especiales.

- VII. El Título VII “Transferencia de Datos” aclara que el Responsable del Tratamiento de la base de datos, pública o privada, solo podrá transferir datos contenidos en ellas cuando el Titular haya dado su consentimiento expreso e inequívoco, y se haga sin vulnerar los principios y derechos reconocidos en esta Ley y su Reglamento. Asimismo, presenta una serie de causales consideradas excepciones al consentimiento requerido para transferir datos personales.
  
- VIII. El Título VIII “Disposiciones sectoriales”. Este Título se divide en dos capítulos y establece cuales son los requisitos para la creación de bases de datos del Sector Público y del Sector Privado, además de otras cuestiones relativas a la aplicaciones de Ley en algunas bases de datos concretas, como las de la agencia tributaria.
  
- IX. El Título IX “De los Mecanismos de Vigilancia y Sanción”, detalla el rol que tiene el IAIP en materia de protección de datos personales, ahora considerado no solo Instituto de Acceso a la Información Pública, sino también de Protección de Datos Personales –siguiendo la línea de su referente normativo mexicano, el IFAI. También detalla el procedimiento que el Titular del Dato Personal debe evacuar ante el IAIP, una vez el Responsable del Tratamiento no ha respetado sus derechos. También hace una tipificación de las faltas, desde las leves a las muy graves, brindando una descripción sobre lo que consiste cada una.
  
- X. El Título X “De la Acción del Hábeas Data” viene a proponer un esquema procesal para interponer el recurso de Hábeas Data que venga a complementar lo dispuesto en la Ley sobre Justicia Constitucional. Lo anterior, previendo necesario que se realicen reformas a la Constitución de la República y la Ley Sobre Justicia Constitucional, para dar mayor peso jurídico a la Ley de Protección de Datos Personales y Acción de Hábeas Data.
  
- XI. El Título XI “Cánones”, propone que la inscripción de base de datos en el IAIP tenga consigo el pago de cánones en la búsqueda de sostenibilidad financiera e inversión continua en tecnología.

El Anteproyecto, concluye especificando una serie de acciones transitorias para preparar el camino hacia la implementación de la Ley de Protección de Datos Personales y Acción de Hábeas Data, tal como la elaboración del Reglamento de la Ley y la conformación e integración de la Gerencia de Protección de Datos (PRODATOS) en el IAIP y el plazo de adecuación para los responsables de bases de datos públicas y privadas.

## **CONTENIDO**

**CONSIDERANDO:** Que la intimidad como derecho fundamental es reconocido en los instrumentos internacionales relativos a los Derechos Humanos ratificados por Honduras, entre estos el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos, al disponer que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, que nadie puede ser objeto de injerencias arbitrarias o ilegales en su vida privada, la de su familia, ni de ataques a su honra o reputación, y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques.

**CONSIDERANDO:** Que la Constitución de la República establece que la persona humana es el fin supremo de la sociedad y del Estado. Todos tienen la obligación de respetarla y protegerla.

**CONSIDERANDO:** Que la Constitución de la República garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

**CONSIDERANDO:** Que ante los avances sociales, económicos y tecnológicos globalizadores a que Honduras es parte, es imperante que el Estado de Honduras establezca unos niveles de protección adecuados de datos personales registrados en bases de datos para garantizar el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

**CONSIDERANDO:** Que el Instituto de Acceso a la Información Pública, es el órgano responsable de la protección de datos personales y establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias y entidades.

### **TÍTULO I DISPOSICIONES GENERALES CAPÍTULO ÚNICO**

#### **Artículo 1.- Objeto y fin**

La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

## **Artículo 2.- Ámbito de aplicación**

Esta Ley será de aplicación a los datos personales registrados en bases de datos automatizadas o manuales, de organizaciones del sector público como del sector privado, y a toda modalidad de uso posterior de estos datos.

El régimen de protección de datos personales que se establece en la presente Ley no será de aplicación:

- a) A las bases de datos mantenidas por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas.
- b) Las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
- c) Las bases de datos creadas y reguladas por leyes especiales.
- d) Las bases de datos y archivos de información periodística y otros contenidos editoriales.

## **Artículo 3.- Definiciones**

- a) **Aviso de Privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el Responsable del Tratamiento que es puesto a disposición del Titular, previo al tratamiento de sus datos personales.
- b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento o procesamiento, automatizado o manual, cualquiera que sea la modalidad de su elaboración, organización o acceso;
- c) **Consentimiento:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el Titular consienta el tratamiento de datos personales que le concierne.
- d) **Datos personales:** Cualquier dato relativo a una persona natural identificada o identificable;
- e) **Datos sensibles:** Aquellos que se refieran a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como: Los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud, físicos o psíquicos y preferencias sexuales u otras análogas que afecten su intimidad, así como cualquier otra información excluida por ley; y, cualquier otro dato respecto de la libertad individual que violente el derecho al honor, a la intimidad personal, familiar y a la propia imagen, consagrado en la Constitución de la República o en convenios internacionales suscritos por Honduras.

- f) **Derecho fundamental a la protección de datos:** Es el derecho que toda persona tiene a controlar sus datos personales que se encuentran registrados en bases de datos de entidades públicas o privadas, personas naturales o jurídicas.
- g) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en conjunto con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- h) **IAIP:** Instituto de Acceso a la Información Pública y Protección de Datos Personales a que hace referencia la Ley de Transparencia y Acceso a la Información Pública.
- i) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en conjunto con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- j) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- k) **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, el almacenamiento, la modificación, la extracción, la consulta, la utilización, la comunicación por transferencia, 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.

## TÍTULO II

### PRINCIPIOS Y DERECHOS BÁSICOS PARA LA PROTECCIÓN DE DATOS PERSONALES

#### CAPÍTULO I

##### PRINCIPIOS RECTORES

**Artículo 4. Principios para la protección de datos personales.** La actuación de los responsables de las bases de datos o de los tratamientos, tanto públicos como privados, y, en general, de todos quienes actúan en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales, los cuales se han de aplicar, de manera armónica e integral:

- a. **Principio de lealtad y legalidad:** Los datos personales no se recolectaran ni elaborarán con procedimientos desleales o ilícitos, ni se utilizarán con fines contrarios a los propósitos establecidos por esta Ley y demás normativa aplicable.



- b. Principio de exactitud:** Los datos personales que se recolecten deberán ser exactos, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieran obtenido.

El Responsable del Tratamiento o del Encargado del Tratamiento tendrá la obligación de verificar la exactitud y pertinencia de los datos registrados y tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas.

- c. Principio de finalidad:** El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del Responsable del Tratamiento o del Encargado del Tratamiento, debiendo limitarse al cumplimiento de las finalidades previstas en la presente Ley.

Si el Responsable del Tratamiento pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos inicialmente comunicados, se requerirá obtener nuevamente el consentimiento del Titular.

No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

- d. Principio de acceso a información:** Los datos personales deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso a información de su Titular. En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- e. Principio de consentimiento:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- f. Principio de no discriminación:** No deberán registrarse datos sensibles que puedan originar una discriminación ilícita o arbitraria, en particular información que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

- g. Principio de seguridad:** La información sujeta a tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, se deberá manejar con las medidas

técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- h. Principio de Responsabilidad:** El Responsable del Tratamiento o Encargado del Tratamiento deberán adoptar las medidas necesarias para cumplir con los principios y obligaciones de la presente Ley y dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante el **IAIP** en el ejercicio de sus competencias y facultades.

## **CAPÍTULO II DERECHOS DEL TITULAR DE LOS DATOS**

**Artículo 5. Derechos frente a la recolección.** Cuando se recojan datos, el Titular tiene el derecho de ser informado, previamente en forma expresa, precisa e inequívoca la información que se recaba de él o ella y con qué fines, a través del **aviso de privacidad**.

**Artículo 6. Contenido del Aviso de Privacidad.** El aviso de privacidad deberá contener, al menos, la siguiente información:

- a. La identidad y domicilio del Responsable que recoge los datos;
- b. Las finalidades del tratamiento de datos y quienes podrán ser sus destinatarios;
- c. Las opciones y medios que el Responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- d. Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud
- e. Los medios para ejercer los derechos de acceso, rectificación, eliminación u oposición, de conformidad con lo dispuesto en esta Ley;
- f. En su caso, las transferencias de datos que se efectúen, y
- g. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

**Artículo 7.- Mecanismos de comunicación.** El aviso de privacidad debe ponerse a disposición del Titular a través de **formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología**, de la siguiente manera:

- a. Cuando los datos personales hayan sido obtenidos personalmente del Titular, el aviso de privacidad deberá ser facilitado en el momento en que se recolecte el dato de forma clara y

fehaciente, a través de los formatos establecidos, salvo que se hubiera facilitado el aviso con anterioridad, y

- b. Cuando los datos personales sean obtenidos directamente del Titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el Responsable del Tratamiento deberá proporcionar al Titular de manera inmediata, la información a que se refiere el artículo anterior.

Cuando los datos personales no hayan sido recolectados del Titular, el Responsable del Tratamiento deberá darle a conocer el cambio en el aviso de privacidad, dentro de los 30 días calendario, siguientes al momento del registro de los datos.

Cuando resulte imposible dar a conocer el aviso de privacidad al Titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del IAIP, el responsable podrá instrumentar medidas compensatorias en términos del Reglamento de esta Ley.

**Artículo 8.- Excepción al consentimiento previo del titular.** No será necesario el consentimiento previo e informado cuando:

- a. Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación;
- b. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
- c. Se trate de listados cuyos datos se limiten en el caso de personas naturales a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento;
- d. Deriven de una relación contractual, científica o profesional del Titular de los datos, y sean necesarios para su desarrollo o cumplimiento;
- e. Se realice por personas naturales o jurídicas, privadas o públicas su uso exclusivo, personal o doméstico.

**Artículo 9.- Derecho de acceso a datos personales.** Todo Titular de datos, tendrá derecho a obtener toda la información concerniente a sí mismo que se encuentre en bases de datos públicas o privadas. Este derecho de acceso a datos personales será ejercido en forma gratuita, **debiendo cubrir el Titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.**

**Artículo 10.- Derechos de rectificación y eliminación.** Todo Titular tendrá derecho a solicitar la rectificación y eliminación de sus datos personales cuando se hayan tratado con infracción a las disposiciones de la presente Ley, en particular a causa del carácter incompleto o inexacto de los datos que induzcan a error, o hayan sido recopilados sin autorización del Titular.

La eliminación de datos personales dará lugar a un **periodo de bloqueo tras el cual se procederá a la supresión del dato**. El Responsable del Tratamiento podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o eliminación y sigan siendo tratados por terceros, el Responsable del Tratamiento deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

**Artículo 11.-Derecho de oposición.** El Titular podrá oponerse al tratamiento de sus datos personales cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

El Titular podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basadas únicamente en un tratamiento automatizado de datos personales, excepto cuando la decisión hubiese sido expresamente solicitada por el Titular; o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre el Responsable del Tratamiento y el Titular. En este último caso, el Titular debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el Tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre el Responsable del Tratamiento por la legislación nacional aplicable.

**Artículo 12.-Derecho referente a la transferencia de datos.** El Responsable del Tratamiento de la base de datos, pública o privada, solo podrá transferir datos contenidos en ellas cuando el Titular haya dado su consentimiento expreso e inequívoco y se haga sin vulnerar los principios y derechos reconocidos en esta Ley y su Reglamento.

El consentimiento para la transferencia de los datos personales puede ser revocado por parte del Titular.

**Artículo 13.- Derecho de Indemnización.** El Titular que considere que ha sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente Ley por el Responsable del Tratamiento o el Encargado del Tratamiento, podrá ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.

**Artículo 14.- Excepciones a los principios y derechos para la protección de datos personales.** Los principios, los derechos y las garantías aquí establecidas podrán ser limitados de manera justa, razonable de acorde con el principio de proporcionalidad, cuando se persigan los siguientes fines:

- 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. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
- e. 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.
- f. La adecuada prestación de servicios públicos.
- g. La eficaz actividad ordinaria de la Administración, por parte de las autoridades públicas.

### **TÍTULO III**

#### **PROCEDIMIENTOS PARA HACER EFECTIVOS LOS DERECHOS**

##### **CAPÍTULO ÚNICO**

**Artículo 15.- Ejercicio de los derechos de acceso, rectificación, eliminación y oposición.** El Titular, o en su caso su representante legal o herederos, podrá ejercer los derechos de **acceso, rectificación, eliminación u oposición** previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Todo Responsable del Tratamiento deberá designar a una persona, o departamento de datos personales, quien dará trámite a la solicitud del Titular o su representante legal, para el ejercicio de los derechos a que se refiere la presente Ley.

**Artículo 16.- Contenido de la solicitud de acceso.** La solicitud de acceso, rectificación, actualización, eliminación u oposición se podrá presentar de manera escrita o por medio electrónico, conteniendo como mínimo, lo siguiente:

- a. El nombre del Titular y domicilio y medio para comunicarle la respuesta a su solicitud, ya sea escrito o electrónico;
- b. Los documentos que acrediten la identidad o, en su caso, la representación legal del Titular;
- c. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y

- d. Cualquier otro elemento o documento que facilite la localización de los datos personales.

**Artículo 17.- Entrega de información sobre datos personales.** La información solicitada, ha de ser proporcionada por el Responsable del Tratamiento dentro de los **diez (10) días hábiles** de haber sido solicitada, entregándose en forma inteligible, empleando para ello un lenguaje claro y sencillo.

Cuando no fuere posible atender la solicitud de acceso a datos personales dentro de dicho plazo, se informará al Titular o representante legal, expresando los motivos del retraso y señalando la fecha en que se atenderá la solicitud, la cual en ningún caso podrá superar **los diez (10) días hábiles siguientes al vencimiento del primer plazo**.

Sin perjuicio de lo que disponga la regulación aplicable a datos relativos a la actividad comercial o crediticia, la solicitud de acceso a datos personales almacenados en una base de datos solamente se podrá realizar en intervalos de **seis (6) meses calendario**, salvo que el Titular haga constar en su solicitud un interés legítimo.

**Artículo 18.- Procedimiento de rectificación, eliminación u oposición.-** El Titular que considere que sus datos personales almacenados en una base de datos debe ser objeto de rectificación, actualización o eliminación, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta Ley, presentará una **solicitud ante el Responsable del Tratamiento**, la cual será tramitado bajo las siguientes reglas:

- a. La **solicitud** ha de cumplir con las formalidades establecidas en el **artículo 15** de la presente Ley. En el caso de solicitudes de rectificación de datos personales, el Titular deberá indicar, las modificaciones a realizarse y aportar la documentación que sustente su petición
- b. Si la **solicitud** resulta incompleta, se requerirá al interesado dentro de los **tres (3) días hábiles** siguientes para que subsane con la información faltante. Transcurridos **dos (2) meses calendario** desde la fecha del requerimiento, sin que el interesado presente la información requerida, se entenderá que ha desistido dicha solicitud.
- c. Una vez recibida **solicitud** completa, el Responsable del Tratamiento incluirá en la base de datos una leyenda que diga "**solicitud en trámite**" y el motivo del mismo, en un término no mayor a **tres (3) días hábiles**. Dicha leyenda deberá mantenerse hasta que la **solicitud** sea resuelta.
- d. El plazo para atender la **solicitud** será de **diez (10) días hábiles** contados a partir del siguiente día hábil que la información se encuentre completa. Cuando no fuere posible atender el **solicitud** dentro de dicho término, se informará al interesado los motivos del retraso y la fecha en que se atenderá su **solicitud**, la cual en ningún caso podrá superar **los diez (10) días hábiles siguientes al vencimiento del primer plazo**.
- e. El Responsable del Tratamiento comunicará al Titular, en un plazo máximo de **veinte (20) días hábiles**, contados a partir de la fecha en que se recibió la solicitud de rectificación,

actualización, eliminación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los **diez (10) días** hábiles siguientes a la fecha en que se comunica la respuesta.

Cuando los datos personales hubiesen sido transferidos con anterioridad a la fecha de rectificación o eliminación y sigan siendo tratados por terceros, el Responsable del Tratamiento deberá hacer de su conocimiento dicha solicitud de rectificación o eliminación al tercero, para que proceda a efectuarlo también.

**Artículo 19.- Denegación justificada al acceso, rectificación, eliminación u oposición.** El Responsable del Tratamiento podrá negar el acceso a los datos personales, o a realizar la rectificación, actualización o conceder la oposición al Tratamiento de los mismos, en los siguientes supuestos:

- a. Cuando el solicitante no sea el Titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
- b. Cuando en su base de datos, no se encuentren los datos personales del solicitante;
- c. Cuando se lesionen los derechos de un tercero;
- d. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, eliminación u oposición de los mismos, y
- e. Cuando la rectificación, eliminación u oposición haya sido previamente realizada.

En todos los casos anteriores, el Responsable del Tratamiento deberá informar el motivo de su decisión y comunicarla al Titular, o en su caso, al representante legal, **en un plazo no mayor a diez (10) días hábiles**, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el Responsable del Tratamiento efectuará el **acceso, rectificación, eliminación u oposición** requerida por el Titular.

## **TÍTULO IV DEBERES DE LOS RESPONSABLES**

### **CAPÍTULO ÚNICO**

**Artículo 20. Deber del Responsable del Tratamiento.** El Responsable del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley y su Reglamento:

- a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho fundamental de protección de datos personales;
- b. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud del consentimiento otorgado;
- c. Cumplir con las obligaciones en torno al aviso de privacidad;
- d. Informar a solicitud del Titular sobre el uso dado a sus datos.
- e. Tramitar las solicitudes de acceso, rectificación, eliminación u oposición en los términos señalados en la presente Ley;
- f. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- g. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- h. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas los cambios respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada;
- i. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
- j. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente Ley y su Reglamento;
- k. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- l. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la solicitud y no haya finalizado el trámite respectivo;
- m. Implementar un **manual de políticas y procedimientos** para garantizar el adecuado cumplimiento de la presente Ley;
- n. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por el **IAIP**;
- o. Informar al **IAIP**, cuando se le presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, y
- p. Cumplir las instrucciones y requerimientos que imparta el **IAIP**.

**Artículo 21.- Deberes de los Encargados del Tratamiento.** Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley y su Reglamento:

- a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho fundamental de protección de datos personales;
- b. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;



- c. Realizar oportunamente la actualización, rectificación o eliminación de los datos en los términos de la presente Ley;
- d. Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco **(5) días hábiles** contados a partir de su recibo;
- e. Implementar un **manual de políticas y procedimientos** para garantizar el adecuado cumplimiento de la presente Ley;
- f. Registrar en la base de datos la leyenda "**solicitud en trámite**" en la forma en que se regula en la presente Ley;
- g. Insertar en la base de datos la leyenda "**información en revisión judicial**" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
- h. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por el **IAIP**;
- i. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
- j. Informar al **IAIP**, cuando se le presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, y
- k. Cumplir las instrucciones y requerimientos que imparta el **IAIP**.

**TÍTULO V**  
**SEGURIDAD DE DATOS**  
**CAPÍTULO ÚNICO**

**Artículo 22.- Seguridad de los datos.** El Responsable del Tratamiento deberá adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta Ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.

Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos, y de las personas que intervengan en la recolección, almacenamiento y uso de los datos.

**Artículo 23.- Deber de confidencialidad.** El Responsable del Tratamiento y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevada del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

**Artículo 24.- Manual de políticas y procedimientos.** Las personas naturales y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y tratamiento de datos personales, emitirán un manual de políticas y procedimientos en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las disposiciones previstas en esta Ley, su Reglamento y demás normativa aplicable.

Para que sea válido, el manual de políticas y procedimientos deberá ser inscrito, así como sus posteriores modificaciones, ante el IAIP.

El IAIP podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos del manual.

## **TÍTULO VI**

### **CATEGORIAS ESPECIALES DE DATOS**

#### **CAPÍTULO ÚNICO**

**Artículo 25.- Datos sensibles.** Toda persona tiene derecho a que se respete su honor, intimidad personal, familiar y a su propia imagen. Ninguna persona puede ser obligada a proporcionar datos personales que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, así como los relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

**Artículo 26.- Tratamiento de datos sensibles.** Los datos sensibles podrán ser objeto de Tratamiento cuando:

- a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, el representante legal del Titular deberá otorgar su autorización.
- c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones, organizaciones no gubernamentales y otras

entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

- d) El Tratamiento de los datos se realice con finalidades estadísticas o científicas cuando se disocien de su Titular.
- e) El Tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la prestación de servicios de salud, siempre que dicho tratamiento de datos se realice por un profesional de la salud sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
- f) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

**Artículo 27.- Datos relativos a las telecomunicaciones.-** Los operadores autorizados para prestar a terceros servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos conforme la presente Ley.

Asimismo, deberán adoptar las medidas técnicas y procesos adecuados para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por esta Ley. En caso que exista un riesgo particular de violación de la seguridad de la red pública, el operador que explote dicha red o preste servicios de telecomunicaciones informará a los abanados sobre dicho riesgo y las medidas a adoptar.

La regulación contenida en esta Ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionada con la seguridad pública y la defensa nacional.

**Artículo 28.- Datos relativos a bases de datos con fines de publicidad.** En la recopilación de información sobre direcciones, reparto de documentos, publicidad, venta y otras actividades similares, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitir establecer hábitos de consumo, cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por el propio Titular u obtenidos con su consentimiento.

Cuando los datos procedan de fuentes accesibles al público, en cada comunicación que se dirija al Titular se informará del origen de los datos y de la identidad del Responsable del Tratamiento, así como de los derechos que le asisten.

En los supuestos contemplados en el presente artículo, el Titular de los datos podrá ejercer los derechos de acceso, actualización o eliminación sin cargo alguno.

**Artículo 29.- Datos relativos a la actividad comercial o crediticia.** El Tratamiento de los datos personales referentes al historial o comportamiento crediticio se regirá por las normas del Sistema Financiero Nacional, sin que esto impida el pleno ejercicio de los derechos frente a la recolección, acceso, rectificación, actualización, eliminación y oposición que establece esta Ley y la Constitución de la República.

Quienes se dediquen a la prestación de servicios de información sobre la solvencia financiera o crediticia únicamente podrán tratar datos personales obtenidos de los registros y las fuentes accesibles al público en general o procedentes del consentimiento informado, expreso e inequívoco del Titular. **De tal manera que el Responsable del Tratamiento debe atender el derecho frente a la recolección que establece el artículo 5 de la presente Ley.**

Cuando el Titular lo solicite, el Responsable del Tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos **seis (6) meses calendario** y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

## TÍTULO VII

### TRANSFERENCIA DE DATOS

#### CAPÍTULO ÚNICO

**Artículo 30.- Transferencia de datos a terceros.** Los datos personales objeto del Tratamiento sólo podrán ser transferidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del transferente y del receptor, con el previo consentimiento expreso del Titular.

**Artículo 31.- Nulidad del consentimiento del titular.** Será nulo el consentimiento para la transferencia de datos personales a un tercero, cuando la información que se le facilita al Titular por parte del Responsable del Tratamiento, no le permita conocer la finalidad o finalidades que tendrán sus datos personales al ser transferidos a un tercero o la actividad que realiza éste.

**Artículo 32.- Excepciones al consentimiento para transferir datos personales.** El consentimiento exigido no será necesario cuando:

- a. La transferencia es autorizada por una ley;
- b. Se trata de datos recolectados a través de fuentes accesibles al público;
- c. El Tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho Tratamiento con base de datos de terceros;
- d. La transferencia que deba efectuarse tenga por destinatario la Policía Nacional, el Ministerio Público o el Poder Judicial, en el cumplimiento de sus atribuciones según ley;

- e. La transferencia se produzca entre organismos del sector público y tenga por objeto el Tratamiento posterior de los datos con fines históricos, estadísticos y científicos, y
- f. La transferencia de datos personales relativos a la salud es necesaria para atender una emergencia que requiera acceder a una base de datos o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud pública.

**Artículo 33.- Cumplimiento legal por cuenta de terceros.** El tercero a que se le transfieran los datos personales, se obliga, por el solo hecho de la transferencia, a la observancia de las disposiciones de la presente Ley.

No se considerará transferencia de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al Responsable del Tratamiento.

**Artículo 34.- Tratamiento de datos por terceros.** La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del Tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los transferirá, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el Título V de la presente Ley que el Encargado del Tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al Responsable del Tratamiento, al igual que cualquier soporte o documentos en que conste algún dato personal objeto del tratamiento.

En el caso de que el Encargado del Tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también como responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

**Artículo 35.- Transferencia de datos a nivel internacional.** Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional en la materia.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por el **IAIP** atendiendo a todas las circunstancias que concurren en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que

se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Sin perjuicio de lo dispuesto en el primer y segundo párrafo del presente artículo, el **IAIP** podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el Responsable de Tratamiento ofrezca garantías respecto a la protección de la vida, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Dichas garantías podrán derivarse de cláusulas contractuales apropiadas.

**Artículo 36.- Excepción a la prohibición de transferir datos a nivel internacional.** La prohibición mencionada en el primer párrafo del artículo anterior, no se será aplicable cuando:

- a. El Titular haya dado su autorización explícita a dicho Tratamiento;
- b. Se requiere el intercambio de datos de carácter médico para atender el tratamiento médico del Titular;
- c. Se realicen transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulta aplicable;
- d. La transferencia sea necesaria para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento o para la ejecución de medidas precontractuales tomadas a petición del Titular;
- e. La transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del Titular, entre el Responsable del Tratamiento y un tercero;
- f. La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial;
- g. La transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta;
- h. Se realiza en el marco de la cooperación judicial internacional, y
- i. En el cumplimiento de acuerdos, tratados o convenios en el marco de tratados internacionales en los cuales la República de Honduras sea parte;

## TÍTULO VIII

### DISPOSICIONES SECTORIALES

#### CAPÍTULO I

##### BASES DE DATO DE TITULARIDAD PÚBLICA

**Artículo 37.- Creación, modificación o eliminación.** La creación, modificación o eliminación de bases de datos pertenecientes a organismos del sector público deberá registrarse en el **IAIP**.

Asimismo, el organismo público deberá comunicar los cambios que se produzcan en la finalidad de la base de dato, en su Responsable del Tratamiento y en la dirección de su ubicación.

Para la eliminación de las bases de datos, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

**Artículo 38.- Registro de bases de datos de organismos del sector público.** Por vía Reglamento se procederá a la regulación detallada de los distintos extremos que deba contener el registro, entre los cuales figurarán:

- a. El organismo público responsable de la base de datos;
- b. La finalidad de la base de datos;
- c. Las personas o colectivos sobre los que se pretenda obtener datos personales o que resulten obligados a suministrarlos;
- d. Los procedimientos de recolección de los datos personales y tratamiento de estos;
- e. La estructura básica de la base de datos y la descripción de los tipos de datos personales incluidos en ella;
- f. Las medidas de seguridad y de confidencialidad;
- g. El destino de los datos y personas naturales o jurídicas a las que pueden ser transferidos los datos personales;
- h. Tiempo de conservación de los datos personales;
- i. La instancia interna donde se presentará y dará trámite a las solicitudes de acceso, rectificación, actualización, eliminación y oposición;
- j. Forma y condiciones en que el Titular puede acceder a sus datos personales y los procedimientos a realizar la rectificación o actualización de los datos, y
- k. En su caso, las transferencias de datos que se prevean a países terceros u organismos internacionales.

**Artículo 39.- Base de datos de las Fuerzas Armadas y operadores de justicia.** Las bases de datos con datos personales creados para  **fines administrativos**  por parte de las Fuerzas Armadas, la Policía Nacional, el Ministerio Público y el Poder Judicial, estarán sujetas a las disposiciones de la presente Ley.

La recolección y tratamiento para fines de investigación y represión del delito de datos personales, sin consentimiento del Titular están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la investigación y represión del delito, debiendo ser almacenados en bases de datos específicas establecidas al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

Los datos personales registrados con fines de investigación se eliminarán cuando no sean necesarios para las averiguaciones que motivaran su recolección y almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

**Artículo 40.- Excepciones a los derechos de acceso, rectificación y eliminación.** El Responsable del Tratamiento de las bases de datos que contengan los datos a que se refiere el primer párrafo del artículo anterior, podrá denegar el acceso, la rectificación o eliminación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

El Responsable del Tratamiento de las bases de datos de la agencia tributaria estatal, podrá, denegar el ejercicio de los derechos de acceso, rectificación y eliminación cuando pueda obstaculizar las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el Titular esté siendo investigado por la agencia tributaria.

**Artículo 41.- Acción ante la denegatoria por el sector público.** El Titular al que se deniegue total o parcialmente el ejercicio de los derechos de acceso, rectificación y eliminación por parte de un organismo del sector público podrá ponerlo en conocimiento del IAIP, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

**Artículo 42.- Excepciones al derecho frente a la recolección.** Lo dispuesto en el artículo 5 de la presente Ley no será aplicable cuando la información del Titular afecte la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.

## **CAPÍTULO II**

### **BASES DE DATO DE TITULARIDAD PRIVADA**

**Artículo 43.- Creación de bases de datos privadas.** Podrán crearse base de datos de titularidad privada que contengan datos personales cuando resulte necesario para el logro de la actividad u



objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de datos personales.

**Artículo 44.- Registro de bases de datos de titularidad privada.** Toda persona natural o jurídica que proceda a la creación de una base de datos personales y que no sean para un uso exclusivamente individual o doméstico, deberán registrar la base de datos previamente ante el **IAIP**.

Por vía reglamento se procederá a la regulación detallada de los distintos extremos que deba contener la notificación, entre los cuales figurarán:

- a. Identificación de la base de datos y el Responsable de la misma;
- b. La finalidad de la base de datos;
- c. La estructura básica de la base de datos y la descripción de los tipos de datos personales incluidos en ella;
- d. Los procedimientos de la recolección de los datos personales y tratamiento de estos;
- e. Las medidas de seguridad y confidencialidad;
- f. El destino de los datos y personas naturales o jurídicas a las que pueden ser transferidos los datos personales;
- g. Tiempo de conservación de los datos personales;
- h. Forma y condiciones en que el Titular puede acceder a sus datos personales y los procedimientos a realizar la rectificación o actualización de los datos.
- i. En su caso, las transferencias de datos que se prevean a países terceros.

## **TÍTULO IX**

### **DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN**

#### **CAPÍTULO I**

#### **DEL INSTITUTO DE ACCESO A LA INFORMACION PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES**

**Artículo 45.- Autoridad de Protección de Datos.** Para los objetivos y propósitos de la presente Ley, el **Instituto de Acceso a la Información Pública y de Protección de Datos Personales (IAIP)** es el responsable de promover y garantizar el derecho fundamental de protección de datos personales y ejercer la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y su Reglamento.

Le corresponderá al IAIP adoptar las resoluciones, elaborar los reglamentos y las demás disposiciones pertinentes para asegurar la correcta aplicación de la presente Ley y su Reglamento. Para tal fin, el IAIP, creará la **Gerencia de Protección de Datos Personales (PRODATOS)**

**Artículo 46.-Dirección.** PRODATOS estará bajo la dirección, orientación, administración y supervisión de un(a) Gerente el cual será nombrado por el Pleno de los Comisionados del IAIP.

No podrá ser nombrado Gerente de PRODATOS quien sea propietario, accionista, miembro de la junta directiva, gerente, asesor, representante legal o empleado de una empresa dedicada a la recolección o el almacenamiento de datos personales. Dicha prohibición persistirá hasta por dos años después de haber cesado sus funciones o vínculo empresarial.

Estará igualmente impedido quien sea cónyuge o pariente hasta el tercer grado de consanguinidad o afinidad de una persona que esté en alguno de los supuestos mencionados anteriormente.

**Artículo 47.- Funciones.** El IAIP deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente Ley. A tales efectos tendrá las siguientes funciones:

- a. Velar por el cumplimiento de la legislación en materia de protección de datos personales, tanto por parte de personas naturales o jurídicas privadas, como por organismos públicos.
- b. Realizar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de protección de datos.
- c. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;
- d. Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones, entre ello, los manuales utilizados.
- e. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.
- f. Realizar y actualizar un censo de las bases de datos a ser reguladas por la presente Ley, administrar el **Registro Nacional de Protección de Datos**, y emitir las órdenes y los actos necesarios para su administración y funcionamiento.
- g. Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementar campañas de promoción para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

- h. Proporcionar apoyo técnico a las los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;
- i. Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.
- j. Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.
- k. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.

**Artículo 48. El Registro Nacional de Protección de Datos.** El **Registro Nacional de Protección de Datos** será administrado por el IAIP y serán objeto de inscripción:

- a. Las bases de datos gestionadas por organismos del sector público;
- b. Las bases de datos de titularidad privada;
- c. Las autorizaciones a que se refiere la presente Ley;
- d. Los **manuales de políticas y procedimientos** que elaboren e implementen los Responsables del Tratamiento y Encargados de Tratamiento.
- e. Los datos relativos a las bases de datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, eliminación y oposición.

Por vía de Reglamento se regulará el procedimiento de inscripción de bases de datos, tanto del sector público como del privado, en el Registro Nacional de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

**Artículo 49.- Consejo Consultivo de Protección de Datos.-** EL IAIP estará asesorado por un Comité Consultivo que apoyará en materia de desarrollo normativo, regulatorio y tecnológico en torno a la protección de datos personales. El Comité Consultivo estará integrado por representantes de los sectores públicos y privados, en la forma siguiente:

- a. Un experto en la materia, nombrado por el Poder Legislativo;
- b. Un experto en la materia, nombrado por el Poder Ejecutivo;
- c. Un experto en la materia, nombrado por el Poder Judicial;
- d. Un experto en la materia, propuesto por el Consejo Superior de Universidades;
- e. Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente;
- f. Un representante del sector de base de datos de titularidad privada, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente, y
- g. Un representante de una organización de derechos humanos de la sociedad civil, seleccionada del modo que se prevea reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

**Artículo 50.- Promoción y difusión del derecho fundamental de protección de datos.** El IAIP elaborará e implementará una estrategia de comunicación dirigida a permitir que los Titulares conozcan los derechos derivados del manejo de sus datos personales, así como los mecanismos que el ordenamiento prevé para la defensa de tales prerrogativas.

Asimismo, promoverá entre las personas y empresas que recolecten, almacenen o manipulen datos personales, la adopción de prácticas y protocolos de actuación acordes con la protección de dicha información.

## **CAPÍTULO II**

### **DEL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS**

**Artículo 51.- Protección de datos personales.** El Titular podrá presentar una solicitud de protección de datos por la respuesta recibida o falta de respuesta del Responsable de Tratamiento.

La **solicitud de protección de datos** también procederá cuando el Responsable del Tratamiento entregue al Titular los datos personales solicitados en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el Titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

**Artículo 52.- Solicitud de protección de datos personales.** La solicitud de protección de datos podrá interponerse por escrito libre o a través de los formatos, del sistema electrónico que al efecto proporcione el IAIP y deberá contener la siguiente información:

- a. El nombre del Titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay;
- b. El nombre del Responsable del Tratamiento ante el cual se presentó la solicitud de acceso, rectificación, actualización, eliminación u oposición de datos personales;
- c. El domicilio para oír y recibir notificaciones;
- d. La fecha en que se le notificó la respuesta del Responsable del Tratamiento, salvo que el procedimiento inicie con la falta de respuesta, en ese caso, a partir del vencimiento de los **veinte (20) hábiles** para atender la solicitud del Titular por parte del Responsable del Tratamiento;
- e. Los actos que motivan su solicitud de protección de datos, y
- f. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

La forma y términos en que deba acreditarse la identidad del titular o bien, la representación legal se establecerán en el Reglamento.

Asimismo, a la solicitud de protección de datos deberá acompañarse la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. En el caso de falta de respuesta sólo será necesario presentar la solicitud.

**Artículo 53.- Solicitud incompleta.** En caso de que la **solicitud de protección de datos** se encuentre incompleta, se requerirá al interesado dentro de los **tres (3) días** hábiles siguientes a la presentación de la solicitud de protección de datos, por una sola ocasión, para que subsane las omisiones dentro de un plazo de **cinco (5) días hábiles**.

Transcurridos dos **(2) meses calendario** desde la fecha del requerimiento, sin que el interesado presente la información requerida, se entenderá que ha desistido dicha solicitud.

**Artículo 54.- Plazos para solicitar protección de datos personales** El procedimiento se iniciará a instancia del Titular o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La **solicitud de protección de datos** deberá presentarse, dentro de los **quince (15) días siguientes** a la fecha en que se comunique la respuesta al Titular por parte del Responsable del Tratamiento.

En el caso de que el Titular de los datos no reciba respuesta alguna por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo **de veinte (20) días hábiles** a partir de la solicitud que el Titular presentó ante el Responsable del Tratamiento. En este caso, bastará que el Titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, actualización, eliminación u oposición.

**Artículo 55.- Traslado al Responsable del Tratamiento.** Recibida la solicitud de protección de datos, el **IAIP** dará traslado de la misma al Responsable del Tratamiento, para que, en el plazo de **diez (10) días hábiles**, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga, a través de un informe. Junto con las argumentaciones y medios probatorios, adjuntará una **declaración jurada** sobre lo expresado y entregado. La omisión de rendir el informe en el plazo estipulado hará que se tengan por ciertos los hechos acusados.

**Artículo 56.- Inspección in situ.** En cualquier momento, el **IAIP** podrá efectuar inspecciones in situ a sus archivos o bases de datos del Responsable del Tratamiento.

**Artículo 57.- Conciliación.** El **IAIP** podrá en cualquier momento del proceso buscar una conciliación entre el Titular de los datos y el Responsable del Tratamiento.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el **IAIP** verificará el cumplimiento del acuerdo respectivo.

Para efectos de la conciliación, se estará al procedimiento que se establezca en el Reglamento de esta Ley.

**Artículo 58.- Plazo para emitir resolución.** El plazo máximo para dictar resolución en el procedimiento de protección de derechos será de **treinta (30) días hábiles**, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, **PRODATOS** podrá ampliar por una vez y hasta por un período adicional de **veinte (20) días hábiles** este plazo.

**Artículo 59.- Resolución favorable al titular.** En caso que la resolución de protección de derechos resulte favorable al Titular de los datos, se requerirá al Responsable del Tratamiento para que, en el plazo de **diez (10) días hábiles** siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento ante el **IAIP** dentro de los siguientes **cinco (5) días hábiles** de su corrección.

Si el Responsable del Tratamiento no cumple íntegramente lo ordenado, estará sujeta a las sanciones previstas en esta y otras leyes.

**Artículo 60.- Publicación de Resoluciones:** Todas las resoluciones del **IAIP** serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al Titular de los datos que lo identifiquen o lo hagan identificable.

### **CAPÍTULO III**

#### **DEL PROCEDIMIENTO DE VERIFICACIÓN**

**Artículo 61.- Verificación.** El **IAIP** verificará el cumplimiento de la presente Ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte.

La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere el Capítulo anterior o se presuma fundada y motivadamente la existencia de violaciones a la presente Ley.

**Artículo 62.-** En el procedimiento de verificación, el **IAIP** tendrá acceso a la información y documentación que considere necesaria, de acuerdo a la resolución que lo motive.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente artículo.

### **CAPÍTULO III DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES**

**Artículo 63.- Imposición de sanciones.** Si con motivo de la evacuación del procedimiento de protección de derechos o del procedimiento de verificación que realice el **IAIP**, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento a que se refiere este Capítulo, a efecto de determinar la sanción que corresponda.

**Artículo 64.- Procedimiento de imposición de sanciones.** El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el **IAIP** al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento y le otorgará un término de **diez (10) días hábiles** para que rinda pruebas y manifieste por escrito lo que a su derecho convenga. En caso de no rendirlas, el **IAIP** resolverá conforme a los elementos probatorios que disponga.

El **IAIP** admitirá las pruebas que estime pertinentes y procederá a su evacuación. Asimismo, podrá solicitar del presunto infractor las demás pruebas que estime necesarias. Concluido la evacuación de las pruebas, el **IAIP** notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los **cinco (5) días hábiles** siguientes a su notificación.

El **IAIP**, una vez analizadas las pruebas y demás elementos que estime pertinentes, resolverá en definitiva dentro de los **treinta (30) días hábiles** a la fecha en que inició el procedimiento sancionador. Cuando haya causa justificada, el **IAIP** podrá ampliar por una vez y hasta por un período adicional de **veinte (20) días hábiles** este plazo.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento de imposición de sanciones, incluyendo presentación de pruebas y alegatos, la celebración de audiencias y el cierre del proceso.

### **CAPÍTULO III DE LAS INFRACCIONES Y SANCIONES**

**Artículo 65.- Faltas leves.** Serán consideradas faltas leves, para los efectos de esta Ley:

- a. Recolectar datos personales sin que se le otorgue suficiente y amplia información al Titular, de conformidad con las disposiciones del artículo 5, y
- b. No cumplir con la solicitud del Titular para el acceso, actualización, rectificación, eliminación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;

**Artículo 66.- Faltas graves.** Serán consideradas faltas graves, para los efectos de esta Ley:

- a. Recolectar, almacenar, transferir o de cualquier otra forma emplear datos personales sin el consentimiento informado e inequívoco del Titular de los datos, con arreglo a las disposiciones de esta ley;
- b. Recolectar, almacenar y transferir datos personales por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos;
- c. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, actualización, eliminación u oposición de datos personales;
- d. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del Responsable del Tratamiento;
- e. Mantener datos personales inexactos cuando resulte imputable al Responsable del Tratamiento, o no efectuar las rectificaciones o eliminaciones de los mismos que legalmente procedan cuando resulten afectados el derecho del Titular;

**Artículo 67.- Faltas muy graves.** Serán consideradas faltas muy graves, para los efectos de esta ley:

- a. Obtener, del Titular o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.
- b. Incumplir el deber de confidencialidad establecido en esta Ley;
- c. Cambiar sustancialmente la finalidad originaria del Tratamiento de los datos, sin respetar el Principio de Consentimiento definido en el artículo 4, inciso e;
- d. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
- e. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
- f. Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme la Ley;
- g. Obstruir los actos de verificación de la autoridad;
- h. Proporcionar a un tercero, información falsa o distinta contenida en un archivo de datos, con conocimiento de ello.
- i. Realizar tratamiento de datos personales sin encontrarse debidamente inscrito ante el IAIP;
- j. Transferir, a las bases de datos de terceros países, información de carácter personal de los hondureños o de los extranjeros radicados en el país, sin el consentimiento de sus titulares.
- k. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el IAIP o los titulares;

**ARTÍCULO 68.- Sanciones.** Si se ha incurrido en alguna de las faltas tipificadas en esta ley, el IAIP impondrá alguna de las siguientes sanciones:

- a. Para faltas menos leves, una multa de **diez (10) a veinte (20) salarios** mínimos.
- b. Para las faltas graves, una multa de **veintiún (21) hasta cuarenta (40) salarios** mínimos.



- c. Para las faltas muy graves, una multa de **cuarenta y un (41) a sesenta (60) salarios mínimos**, y la suspensión para el funcionamiento del fichero de uno a seis meses en el caso de titularidad privada. Para el caso de base de datos del sector pública, el Reglamento establecerá la sanción.

**Artículo 69.- Criterios para imponer sanciones.** El IAIP fundará y motivará sus resoluciones, considerando:

- a. La naturaleza del dato;
- b. La notoria improcedencia de la negativa del Responsable del Tratamiento, para realizar los actos solicitados por el titular, en términos de esta Ley;
- c. El carácter intencional o no, de la acción u omisión constitutiva de la infracción;
- d. La capacidad económica del Responsable del Tratamiento, y
- e. La reincidencia.

**Artículo 70.-** Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte.

## **TÍTULO X DE LA ACCIÓN DE HÁBEAS DATA**

**Artículo 71. Hábeas data.-** Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder.

Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

**Artículo 72.- Procedencia.** El Titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

- a. Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el Responsable del Tratamiento, en las oportunidades y plazos previstos por la ley.
- b. Cuando haya solicitado al Responsable del Tratamiento su rectificación, actualización, eliminación u oposición y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la Ley.

**Artículo 73.- Competencia.** Serán competentes para conocer en las acciones de protección de datos personales o habeas data:

- a. La Sala de lo Constitucional de la Corte Suprema de Justicia, cuando la acción se dirija contra un ente de la Administración Pública, municipalidades y demás entidades del Sector Público.
- b. El Juzgado de Letras de lo Civil con jurisdicción, cuando la acción se dirija contra una persona natural o jurídica con titularidad privada de la base de datos.

**Artículo 74.- Legitimación.** La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado.

**Artículo 75.- Procedimiento.** Las acciones que se promuevan por violación a los derechos contemplados en la presente Ley se regirán por las normas contenidas en los artículos que siguen al presente.

**Artículo 76.- Trámite de primera instancia.** Salvo que la acción fuera manifiestamente improcedente, en cuyo caso el tribunal la rechazará sin sustanciarla y dispondrá el archivo de las actuaciones, se convocará a las partes a una audiencia pública dentro del plazo de tres (3) días hábiles de la fecha de la presentación de la demanda.

En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El tribunal, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad, e interrogará a los testigos y a las partes, sin perjuicio de que aquéllos sean, a su vez, repreguntados por los abogados. En cualquier momento podrá ordenar diligencias para mejor proveer.

La sentencia se dictará en la audiencia o a más tardar, dentro de las veinticuatro horas de su celebración. Sólo en casos excepcionales podrá prorrogarse la audiencia por hasta tres (3) días hábiles.

Las notificaciones podrán realizarse por intermedio de la autoridad policial. A los efectos del cómputo de los plazos de cumplimiento de lo ordenado por la sentencia, se dejará constancia de la hora en que se efectuó la notificación.

**Artículo 77.- Medidas provisionales.** Si de la demanda o en cualquier otro momento del proceso resultare, a juicio del tribunal, la necesidad de su inmediata actuación, éste dispondrá, con carácter provisional, las medidas que correspondieren en amparo del derecho o libertad presuntamente violados.

**Artículo 78.- Contenido de la sentencia.** La sentencia que haga lugar al hábeas data deberá contener:

- a. La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.
- b. La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo.
- c. El plazo para el cumplimiento de lo dispuesto, que será fijado por el tribunal conforme las circunstancias de cada caso, y no será mayor de quince (15) días calendario, computados a partir de la notificación.

**Artículo 79. Recurso de apelación y segunda instancia.** En el proceso de habeas data sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente.

**Artículo 80. Sumariedad. Otros aspectos.-** En los procesos de habeas data no podrán deducirse cuestiones previas, reconveniones ni incidentes. El tribunal, a petición de parte o de oficio, subsanará los vicios de procedimiento, asegurando, dentro de la naturaleza sumaria del proceso, la vigencia del principio de contradictorio.

## **TÍTULO XI CÁNONES**

**ARTÍCULO 83.- Canon por regulación y administración de bases de datos.** Los Responsables del Tratamiento que deban inscribirse ante el **IAIP**, de conformidad con el artículo 48 de esta Ley, estarán sujetos a un canon de regulación y administración de bases de datos que deberá ser cancelado anualmente, con un monto equivalente en a **cien dólares de los Estados Unidos de América (US\$100)**, pagaderos en lempiras a la tasa oficial de venta del Banco Central de Honduras. El procedimiento para realizar el cobro del presente canon será detallado en el Reglamento que a los efectos deberá emitir el **IAIP**.

**ARTÍCULO 84.- Canon por comercialización de consulta.** EL Responsable del Tratamiento de la base de datos deberá cancelar ante el **IAIP** un canon por cada venta de los datos personales, de personas individualizables registradas legítimamente y siempre que sea comercializado con fines de lucro, el cual oscilará entre los veinticinco centavos de dólar (\$0,25) y un dólar (\$1), pagaderos en lempiras a la tasa oficial de venta del Banco Central de Honduras, monto que podrá ser fijado dentro de dicho rango vía reglamento.

En caso de contratos globales de bajo, medio y alto consumo de consultas, o modalidades contractuales de servicio en línea por número de aplicaciones, será el reglamento de la ley el que fije el detalle del cobro del canon que no podrá ser superior al diez por ciento (10%) del precio contractual.

## **TRANSITORIOS**

**PRIMERO.-** La presente Ley entrará en vigencia a partir de su publicación en el Diario Oficial La Gaceta.

**SEGUNDO.-** A partir de la fecha de entrada en vigencia de esta Ley, se iniciará el proceso de conformación e integración de la **Gerencia de Protección de Datos (PRODATOS)**; para ello, se dispondrá de un plazo máximo de **seis (6) meses calendario**.

**TERCERO.-** El Instituto de Acceso a la Información Pública emitirá el Reglamento de esta Ley dentro del año siguiente a su entrada en vigor.

**CUARTO.-** Las personas físicas o jurídicas, públicas o privadas, que en la actualidad son titulares o administradoras de las bases de datos objeto de esta Ley, deberán adecuar sus procedimientos y reglas de actuación, así como el contenido de sus bases de datos a lo establecido en la presente Ley, en un plazo máximo de un año a partir de la creación de la **Gerencia de Protección de Datos (PRODATOS)**.