

CONGRESO DE LA REPÚBLICA  
GUATEMALA, C. A.

DIRECCIÓN LEGISLATIVA  
- CONTROL DE INICIATIVAS -

NÚMERO DE REGISTRO

6464

FECHA QUE CONOCIÓ EL PLENO: 5 DE DICIEMBRE DE 2024.

INICIATIVA DE LEY PRESENTADA POR EL REPRESENTANTE JORGE MARIO VILLAGRÁN ALVAREZ.

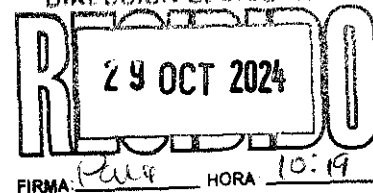
INICIATIVA QUE DISPONE APROBAR LEY DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE DERECHOS DIGITALES.

TRÁMITE: PASE A LA COMISIÓN DE ASUNTOS DE SEGURIDAD NACIONAL PARA SU ESTUDIO Y DICTAMEN CORRESPONDIENTE.



**CONGRESO**  
DE LA **REPÚBLICA**

CONGRESO DE LA REPÚBLICA  
DIRECCIÓN LEGISLATIVA



Guatemala, 24 de octubre de 2024

Magister  
Luis Eduardo López Ramos  
Encargado de Despacho  
Dirección Legislativa  
Su Despacho

Magister López:

De la manera más atenta me dirijo a usted para adjuntarle la Iniciativa de Ley que dispone aprobar "**LEY DE PROTECCION DE DATOS PERSONALES Y GARANTIA DE DERECHOS DIGITALES**", en versión impresa y digital, para el trámite correspondiente.

Me suscribo de usted.

Atentamente,

Diputado Jorge Mario Villagrán Álvarez  
Jefe de Bancada Partido Azul



Cc: file  
Adjunto físico: lo indicado  
Digital: [clopez@congreso.gob.gt](mailto:clopez@congreso.gob.gt)  
JMVA/mdep

## INICIATIVA NUEVA

### EXPOSICIÓN DE MOTIVOS

#### HONORABLE PLENO

La Constitución Política de la República de Guatemala, en el artículo 1, establece que el Estado de Guatemala se organiza para proteger a la persona y a la familia; su fin supremo es la realización del bien común.

*"...la Constitución Política dice en su artículo 1 que el Estado de Guatemala protege a la persona... pero añade inmediatamente que su fin supremo es la realización del bien común, por lo que las leyes... pueden evaluarse tomando en cuenta que los legisladores están legitimados para dictar las medidas que, dentro de su concepción ideológica y sin infringir preceptos constitucionales, tiendan a la consecución del bien común. Al respecto conviene tener presente que la fuerza debe perseguir objetivos generales y permanentes, nunca fines particulares..."<sup>1</sup>*

En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos. El hombre y la mujer, cualquiera que sea su estado civil, tienen iguales oportunidades y responsabilidades. Ninguna persona puede ser sometida a servidumbre ni a otra condición que menoscabe su dignidad. Los seres humanos deben guardar una conducta fraternal entre sí.

"...el principio de igualdad, plasmado en el artículo 4o. de la Constitución Política de la República impone que situaciones iguales sean tratadas normativamente de la misma forma; pero para que el mismo rebase un significado puramente formal y sea realmente efectivo, se impone también que situaciones distintas sean tratadas desigualmente, conforme sus diferencias. Esta Corte ha expresado en anteriores casos que este principio de igualdad hace una referencia a la universalidad de la ley, pero no prohíbe, ni se opone a dicho principio, el hecho que el legislador contemple la necesidad o conveniencia de clasificar y diferenciar situaciones distintas y darles un tratamiento diverso, siempre que tal diferencia tenga una



---

<sup>1</sup> Corte de Constitucionalidad. Gaceta No. 1, expediente No. 12-86, página No. 3, sentencia: 17-09-86.

justificación razonable de acuerdo con el sistema de valores que la Constitución acoge..."<sup>2</sup>

Sobre el derecho de petición, que es un derecho constitucional, se establece en la Constitución Política que los habitantes de la República de Guatemala tienen derecho a dirigir, individual o colectivamente, peticiones a la autoridad, la que está obligada a tramitarlas y deberá resolverlas conforme a la ley. En materia administrativa el término para resolver las peticiones y notificar las resoluciones no podrá exceder de treinta días. En materia fiscal, para impugnar resoluciones administrativas en los expedientes que se originen en reparos o ajustes por cualquier tributo, no se exigirá al contribuyente el pago previo del impuesto o garantía alguna<sup>3</sup>.

El mismo cuerpo legal establece en el artículo 30, que todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia<sup>4</sup>. Así también, que toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos<sup>5</sup>.

Específicamente, en el expediente 1356-2006, la **Corte de Constitucionalidad** ha expresado que *«el amparo resulta ser la acción constitucional idónea para garantizar el derecho que a toda persona asiste de acceder a su información*

---

<sup>2</sup> Corte de Constitucionalidad. Gaceta No. 24, expediente No. 141- 92, página No. 14, sentencia: 16-06-92.

<sup>3</sup> "...De conformidad con lo que establece el artículo 28 de la Constitución, los habitantes de la República tienen el derecho a dirigir, individual o colectivamente, peticiones a la autoridad, la que está obligada a tramitarlas y resolverlas conforme a la ley. Este precepto, en concordancia con el artículo 10 inciso f) de la Ley de Amparo, Exhibición Personal y de Constitucionalidad, establece que en materia administrativa el término máximo para resolver y notificar las resoluciones es el que señala la ley específica aplicable al caso concreto o, en su defecto, el de treinta días. En caso de que la autoridad omita el cumplimiento de la obligación referida en dicho término el interesado puede acudir al amparo para que se fije un plazo razonable a efecto de que cese la demora en resolver y notificar..." Gaceta No. 54, expediente No. 661-99, página No. 296, sentencia: 27-10-99.

<sup>4</sup> Véase: - Gaceta No. 57, expediente No. 438-00, página No. 647, sentencia: 27-09- 00. - Gaceta No. 33, expediente No. 553-93, página No. 175, sentencia: 29-09- 94. - Gaceta No. 13, expediente No. 178-89, página No. 190, sentencia: 13-09- 89. Se menciona en: - Gaceta No. 36, expediente No. 556-94, página No. 64, sentencia: 25-04- 95./ "...La potestad de los administrados de dirigir peticiones a la autoridad, individual o colectivamente, se encuentra garantizada como un derecho subjetivo público en el artículo 28 constitucional. De ello deviene la obligación del órgano ante el cual se formule la solicitud de resolver, acogiendo o denegando la pretensión, dentro del plazo que la ley rectora del acto establece..." Gaceta No.61, expediente No. 1161-00, sentencia: 18-07- 01. Véase: - Gaceta No. 59, expediente No. 782-00, página No. 284, sentencia: 04-01- 01. - Gaceta No. 56, expediente No. 235-00, página No. 510, sentencia: 24-05- 00. - Gaceta No. 50, expediente No. 1028-97, página No. 403, sentencia: 26- 11-98. - Gaceta No. 26, expediente No. 254-92, página No. 59, sentencia: 07-10- 92. Se menciona en: - Gaceta No. 63, expediente No. 1270-01, sentencia: 12-02-02. - Gaceta No. 59, expedientes Nos. 729-00 y 744-00, página No. 515, sentencia: 27-02-01. - Gaceta No. 57, expediente No. 982-99, página No. 13, sentencia: 05-07- 00. - Gaceta No. 56, expediente No. 95-00, página No. 624, sentencia: 21-06- 00. - Gaceta No. 1, expediente No. 12-86, página No. 10, sentencia: 17-09-86.

<sup>5</sup> Se menciona en: - Gaceta No. 57, expediente No. 438-00, página No. 647, sentencia: 27- 09-00.

*personal recabada en bancos de datos o registros particulares u oficiales (...) o cuando esos datos sean proporcionados por personas individuales o jurídicas que prestan un servicio al público de suministros de información de personas, a fin de positivar aquellos derechos de corregir, actualizar, rectificar, suprimir o mantener en confidencialidad información o datos que tengan carácter personal, y así garantizar el adecuado goce de los derechos reconocidos en los artículos 4º, 28 y 31 de la Constitución»*

En el marco del bloque de constitucionalidad, la **Declaración Americana de los Derechos y Deberes del Hombre**, el cual supone una obligación por parte del Estado para facilitar el acceso a información cuando su objeto es el de investigar datos, conductas o políticas públicas.

La **Convención Americana** reconoce y protege el derecho a la privacidad, la honra y la reputación en sus artículos 13.2 y 11. Estos artículos reconocen la importancia del honor y la dignidad individual al establecer la obligación de respetar ambos derechos. Establecen que estos derechos deben estar libres de interferencias arbitrarias o abusivas o ataques abusivos, y que toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques. La privacidad, por lo tanto, es un derecho que tiene toda persona para preservar la vida privada del marco social claramente reconocido por la ley.

En cuanto al artículo 11, aunque la Convención no establece las circunstancias en que este derecho puede ser restringido o limitado, la Corte Interamericana, enunció que el artículo 32.2 de la Convención prescribe las reglas interpretativas a las cuales se suscriben dichas restricciones al establecer: Los derechos de cada persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común, en una sociedad democrática. Por lo tanto, el derecho a la privacidad, de acuerdo con lo estipulado por la Convención, debe dictarse en conformidad con leyes legítimas y su contenido y finalidad deben atender el bien común y ser armonizadas sin limitar indebidamente el derecho a la libertad de expresión en la búsqueda y publicidad de información de interés público, entre otros.

En cuanto a la relación entre el derecho a la verdad y el artículo 13.1 de la Convención Americana, la Comisión Interamericana de Derechos Humanos alegó en el caso Barrios Altos ante la Corte Interamericana que: [...] *El derecho a la verdad se fundamenta en los artículos 8 y 25 de la Convención, en la medida que ambos son "instrumentales" en el establecimiento judicial de los hechos y circunstancias que rodean la violación de un derecho fundamental. Asimismo, [...] este derecho se enraíza en el artículo 13.1 de la Convención, en cuanto reconoce*



*el derecho de buscar y recibir información. [...] en virtud de este artículo, sobre el Estado recae una obligación positiva de garantizar información esencial para preservar los derechos de las víctimas, asegurar la transparencia de la gestión estatal y la protección de los derechos humanos.*<sup>6</sup>

## **I. Acción de Habeas Data**

Una de las formas para garantizar el derecho a la protección contra información abusiva, inexacta o perjudicial de las personas es el acceso a bancos de datos tanto públicos como privados con la finalidad de actualizar, rectificar, anular o mantener en reserva, en caso de que sea necesario, la información del particular interesado. Esta acción conocida como *habeas data* se instituyó como una modalidad del proceso de amparo para proteger la intimidad de las personas. Mediante este procedimiento se garantiza a toda persona a acceder a información sobre sí misma o sus bienes contenida en base de datos o registros públicos o privados, y en el supuesto caso que sea necesario, actualizar, rectificar, anular o mantener en reserva dicha información con la finalidad de proteger ciertos derechos fundamentales.

El principio 3 de la Declaración de Principios sobre Libertad de Expresión de la CIDH establece: toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.

La acción de *habeas data* se erige sobre la base de tres premisas: 1) el derecho de cada persona a no ser perturbado en su privacidad 2) el derecho de toda persona a acceder a información sobre sí misma en bases de datos públicos y privados para modificar, anular o rectificar información sobre su persona por tratarse de datos sensibles, falsos, tendenciosos o discriminatorios y 3) el derecho de las personas a utilizar la acción de *hábeas data* como mecanismo de fiscalización.

Este derecho de acceso y control de datos personales constituye un derecho fundamental en muchos ámbitos de la vida, pues la falta de mecanismos judiciales que permitan la rectificación, actualización o anulación de datos afectaría directamente el derecho a la privacidad, el honor, la identidad personal, la propiedad y la fiscalización sobre la recopilación de datos obtenidos.

---

<sup>6</sup> OEA» CIDH » Relatoría Especial para la Libertad de Expresión » 4 - Capítulo III - Acción de Habeas Data y Acceso a la Información. Disponible en: <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=382&IID=2> Consulta de fecha 15 de agosto de 2024.



Asimismo, esta acción adquiere una importancia aún mayor con el avance de nuevas tecnologías. Con la expansión en el uso de la computación e Internet, tanto el Estado como el sector privado tienen a su disposición en forma rápida una gran cantidad de información sobre las personas. Por lo tanto, es necesario garantizar la existencia de canales concretos de acceso rápido a la información para modificar información incorrecta o desactualizada contenida en las bases de datos electrónicas protegiendo el derecho a la intimidad de los individuos. El derecho a la intimidad es uno de los derechos que se relacionan más directamente con los límites del ejercicio de la libertad de expresión y la libertad de información.

El ataque a la privacidad se realiza generalmente a través de la búsqueda y difusión de información. La Relatoría desea puntualizar que tanto el derecho a la privacidad y la reputación como el derecho de libertad de expresión no son absolutos y deben ser armonizados y balanceados, de forma tal que no desemboquen en la negación de otros derechos.

La acción de *habeas data* impone ciertas obligaciones a las entidades que procesan información: el usar los datos para los objetivos específicos y explícitos establecidos; y garantizar la seguridad de los datos contra el acceso accidental, no autorizado o la manipulación. En los casos en que entes del Estado o del sector privado hubieran obtenido datos en forma irregular y/o ilegalmente, el peticionario debe tener acceso a dicha información, inclusive cuando ésta sea de carácter clasificada con el objeto de devolverle la tutela de la data al individuo que se ve afectado. La acción de *hábeas data* como mecanismo de fiscalización de las entidades de seguridad e inteligencia dentro de este contexto, tiene como finalidad verificar la legalidad en la recopilación de datos sobre las personas. La acción de *hábeas data* habilita al damnificado o sus familiares a tomar conocimiento del objeto de la recopilación y en caso de que estos hayan sido recabados en forma ilegal determinar una posible sanción a los responsables. La publicidad de las prácticas ilegales en la recopilación de datos sobre las personas puede tener un efecto preventivo sobre las prácticas de estas agencias en el futuro.<sup>7</sup>

## II. Protección de datos

La protección de datos se trata de todos aquellos procesos, herramientas y estrategias enfocadas en salvaguardar la información sensible e importante de personas y organizaciones contra todos los agentes externos que puedan usarlos sin consentimiento. Asimismo, busca blindar los datos generados física o



---

<sup>7</sup> Ídem.

informáticamente de prácticas de corrupción, fugas de información o pérdida de datos por negligencia o fallas en el sistema de almacenamiento y gestión de datos.

Cuando se habla de protección de datos, el agente u oficial de protección de datos figura como el responsable de identificar los datos sensibles y diseñar planes y políticas para asegurarlos.

## **II.1 Protección, seguridad y publicidad de datos**

Ahora bien, es muy común pensar que la protección de datos, seguridad de datos y privacidad de datos son la misma cosa. Sin embargo, la realidad es que funcionan como conceptos y disciplinas diferentes para lograr casi el mismo resultado: salvaguardar la información.

Hablar de protección de datos y seguridad de datos es comentar sobre dos conceptos muy diferentes. La seguridad de datos se refiere a todas aquellas estrategias y herramientas utilizadas para identificar y detener ataques contra los datos de una persona, empresa, organización o institución sobre sus recursos de Tecnología de Información. Mientras que, la protección de datos, por su parte, es una metodología creada con el propósito de asegurar que los datos puedan ser recuperados luego de un ataque o una pérdida.

La principal diferencia entre ellos radica que la privacidad de datos tiene como objetivo esencial garantizar el acceso solo a los individuos autorizados para ello. Mientras que la seguridad de datos está enfocada más bien en blindar el sistema de infiltraciones.

En Guatemala está vigente la **Ley de Acceso a la Información Pública, Decreto 57-2008**, la cual establece que es de orden público, de interés nacional y utilidad social; establece las normas y los procedimientos para garantizar a toda persona, natural o jurídica, el acceso a la información o actos de la administración pública que se encuentre en los archivos, fichas, registros, base, banco o cualquier otra forma de almacenamiento de datos que se encuentren en los organismos del Estado. Esta ley es importante, pero distinta a la presente iniciativa de ley.

El Decreto 57-2008, regula específicamente que los sujetos obligados deberán mantener, actualizada y disponible, en todo momento, de acuerdo con sus funciones y a disposición de cualquier interesado, con esto se refiere a la siguiente información, que puede ser consultada de manera directa o a través de los portales electrónicos de cada sujeto obligado: 1. Estructura orgánica y funciones de cada una de las dependencias y departamentos, incluyendo su marco





normativo; 2. Dirección y teléfonos de la entidad y de todas las dependencias que la conforman; 3. Directorio de empleados y servidores públicos, incluyendo números de teléfono y direcciones de correo electrónico oficiales no privados; quedan exentos de esta obligación los sujetos obligados cuando se ponga en riesgo el sistema nacional de seguridad, la investigación criminal e inteligencia del Estado; 4. Número y nombre de funcionarios, servidores públicos, empleados y asesores que laboran en el sujeto obligado y todas sus dependencias, incluyendo salarios que corresponden a cada cargo, honorarios, dietas, bonos, viáticos o cualquier otra remuneración económica que perciban por cualquier concepto. Como se puede apreciar, *strictu sensu*, el objeto de esa ley es garantizar la transparencia de la administración pública, de los sujetos obligados y el derecho de toda persona a tener acceso libre a la información pública y para ello establece principios y el procedimiento para la solicitud y entrega de la información.

## **II.2. Importancia de la protección de datos**

Teniendo en cuenta los grandes riesgos que implican la manipulación de las bases de datos de empresas, instituciones y organizaciones, cada una de ellas está en la obligación de establecer mecanismos de resguardo y protección de cada una de las piezas de información. A esto, se le suma la innegable competitividad que existe en casi todos los sectores.

Ahora bien, también es justo decir que el principal motivo por el cual la protección de datos dejó de ser una herramienta y se convirtió en una obligación es precisamente el cumplimiento de leyes más garantistas en países de todo el mundo.<sup>8</sup>

## **II.3. Riesgos relacionados a datos desprotegidos**

Toda empresa o institución tiene en su poder documentos tributarios como facturas o recibos, información de clientes como nombres o emails, información de nómina como números de cuenta bancaria o direcciones personales, etc.

Si a esto le sumamos la influencia de herramientas digitales como el Big Data, que es capaz de leer millones de kilobytes de data en línea y las técnicas innovadoras que usan los cibercriminales para fugar esta información, es importante considerar los riesgos.<sup>9</sup>



---

<sup>8</sup> Disponible en: <https://www.sydie.com/es/blog/proteccion-de-datos-que-es-y-como-funciona-en-los-contextos-empresarial-y-personal-635c9031dd972c188d314148> consulta de fecha 15 de agosto de 2024.

<sup>9</sup> Idem.

de los datos personales, reduciendo los riesgos asociados a la economía digital.

6. **Transparencia y Responsabilidad:** la normativa promoverá la transparencia en el tratamiento de datos personales y la rendición de cuentas por parte de las entidades responsables, mejorando la gestión y el manejo de la información.

## **II.5. Derecho comparado**

Gracias a la influencia de la Unión Europea y su preocupación por el respeto a la vida privada de sus habitantes, el 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos de la UE, generando una transformación en las normativas de múltiples países, incluidos los latinoamericanos. A continuación, se presenta algunos de estos avances:

- **España:** La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que la ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Protege los datos de las personas vivas y fallecidas, establece principios. Así mismo, regula el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos y el consentimiento de los datos, incluyendo de menores de edad, etc.

- **México:** En México entró en vigor la Ley Federal de protección de datos personales en posesión de los particulares en 2010. En ella las organizaciones e instituciones privadas que obtengan, almacenen, usen o transfieran información de los usuarios deben cumplir ciertas obligaciones. En este caso el responsable, que toma las decisiones sobre el tratamiento de la información, debe cumplir con ocho principios:

- Licitud: cumpliendo las normativas de la ley.
- Consentimiento: obteniendo los datos con el consentimiento de los propietarios.
- Información: comunicando las bases sobre el tratamiento de los datos.
- Calidad: asegurando la exactitud, completitud y actualización de los datos.
- Finalidad: apegándose a los objetivos descritos en el aviso de privacidad.
- Lealtad: protegiendo los intereses de los propietarios.
- Proporcionalidad: almacenando y usando solo los datos necesarios para tal fin.



## **II.4. Vulnerabilidades y beneficios**

Las vulnerabilidades y repercusiones del mal manejo de datos personales se pueden enumerar según lo siguiente:


1. Robo de Identidad: Sin medidas adecuadas de protección, los datos personales pueden ser utilizados por delincuentes para cometer fraude, acceder a cuentas bancarias y realizar compras no autorizadas, causando graves perjuicios económicos y legales a las víctimas.
2. Discriminación: El acceso no autorizado a datos sensibles puede llevar a situaciones de discriminación laboral, social o en la prestación de servicios, afectando negativamente la igualdad y los derechos humanos de los ciudadanos.
3. Pérdida de Confidencialidad: La divulgación no autorizada de información personal puede exponer detalles íntimos de la vida de las personas, afectando su privacidad y reputación, y causando daños emocionales y psicológicos.
4. Uso Indebido de Información: Las empresas y entidades pueden utilizar datos personales para fines no autorizados, como el envío de publicidad no deseada, la elaboración de perfiles sin consentimiento o la explotación comercial de la información.

Los beneficios de contar con una ley de protección de datos en Guatemala traerán múltiples beneficios a todos los niveles de la sociedad:

1. Fortalecimiento de la Confianza: Una ley clara y robusta aumentará la confianza de los ciudadanos en el uso de servicios digitales y en la interacción con instituciones públicas y privadas, promoviendo una mayor participación en la economía digital.
2. Seguridad Jurídica: la normativa proporcionará un marco legal que garantizará la seguridad jurídica tanto para los ciudadanos como para las entidades que tratan datos personales, estableciendo derechos, obligaciones y sanciones claras.
3. Protección de Derechos Fundamentales: la ley garantizará el respeto a los derechos fundamentales a la privacidad y a la autodeterminación informativa, protegiendo a los ciudadanos de abusos y mal uso de sus datos personales.
4. Impulso a la Innovación y Competitividad: al establecer estándares de protección de datos, se fomentará la innovación y la competitividad en el sector empresarial, ya que las empresas deberán adoptar mejores prácticas y tecnologías para cumplir con la normativa.
5. Prevención de Abusos y Fraudes: la ley establecerá mecanismos y medidas de seguridad que contribuirán a prevenir abusos, fraudes y cualquier uso indebido



- Responsabilidad: haciéndose responsable por el tratamiento de la información.
- 
- **Colombia:** En Colombia existe la Ley de Protección de Datos Personales, también llamada la Ley 1581 de 2012. En ella se reconoce y se asegura el derecho que tienen las personas de conocer y modificar la información en las bases de datos sobre ellos que haya sido almacenada por organizaciones públicas o privadas.
  - **Perú:** En Perú existe la Ley de Protección de Datos Personales que tiene el propósito de asegurar los derechos fundamentales de las personas a través de un tratamiento adecuado. Esta normativa aplica para todas las instituciones que usen bancos de datos dentro de sus operaciones que se encuentren físicamente en Perú. Las obligaciones que establece a los propietarios de los bancos de datos es un correcto tratamiento de los datos con previo consentimiento del titular; recopilación de datos actualizados, necesarios, pertinentes y adecuados y asegurar los derechos del titular.
  - **Chile:** En Chile existe la Ley de Protección de Datos Personales o Ley 19.628, en la cual se establecen las medidas para el almacenamiento, uso, transferencia y tratamiento de datos con consentimiento previo, informado y escrito por el propietario de estos. Dentro de ella se separan las responsabilidades entre los organismos públicos y privados, donde se encuentra muy por detrás de otros países de la región en cuanto al acoplamiento con el RGPD.<sup>10</sup>
  - **Brasil:** emitió su ley General de Datos de Brasil -LGPD- entró en vigor en agosto de 2020 con un periodo de gracia de 12 meses. Su aplicación comenzó en agosto de 2021 y está dirigida por la Autoridad Nacional de Protección de Datos (ANPD). Las organizaciones que recopilan y tratan datos personales de individuos en Brasil deben familiarizarse con la LGPD y conseguir el cumplimiento. Esta ley, crea nuevos derechos para los interesados:
- Confirmación de la existencia del procesamiento de sus datos
  - Acceso a sus datos
  - Corregir información incompleta, inexacta o desactualizada
  - Anonimizar, bloquear o eliminar datos innecesarios o excesivos que no se estén procesando conforme a la LGPD



<sup>10</sup> Disponible en: <https://www.sydle.com/es/blog/proteccion-de-datos-que-es-y-como-funciona-en-los-contextos-empresarial-y-personal-635c9031dd972c188d314148> consulta de fecha 15 de agosto de 2024.

- Hacer que sus datos sean portables, es decir, que se puedan facilitar a otro servicio o procesador si se solicita
- Que se eliminen sus datos
- Información sobre entidades públicas o privadas con las que el controlador haya compartido datos
- Información sobre la posibilidad de denegar el consentimiento y las consecuencias
- Revocar el consentimiento

Estos derechos tomaron como modelo principalmente los que el RGPD otorga a los ciudadanos europeos y tienen implicaciones directas para los propietarios y operadores de los sitios web por todo el mundo, que recopilan y/o tratan datos de individuos en Brasil.<sup>11</sup>

### **III. Análisis**

La protección de datos personales es crucial para garantizar la privacidad, la dignidad y la autonomía de los individuos. Los datos personales, que incluyen información sensible como el estado de salud, la orientación sexual, las creencias religiosas y las opiniones políticas, son elementos íntimos que, si son mal manejados, pueden tener repercusiones graves en la vida de las personas.

En Guatemala, la Ley de Acceso a la Información Pública, Decreto 57-2008, establece la garantía a la transparencia de la administración pública, de los sujetos obligados y el derecho de toda persona a tener acceso libre a la información pública, pero este derecho se limita a solicitar información de carácter público generada, administrada o en poder de los sujetos obligados.

La presente iniciativa de ley garantiza los derechos fundamentales a la privacidad y autodeterminación informativa, relacionada a las actividades de tratamiento de datos personales realizadas por entidades responsables, ya sea públicas o privadas, dentro o fuera del territorio nacional de la República de Guatemala, principalmente cuando dichas actividades estén relacionadas con la oferta de bienes y servicios a los ciudadanos guatemaltecos o el monitoreo de su comportamiento. A diferencia del Decreto 57-2008, la presente iniciativa de ley llena el vacío legal de una normativa clara y específica sobre protección de datos



---

<sup>11</sup> Idem.

personales que han sido utilizados de manera indebida por no contar con un marco regulatorio.

En la era digital actual, los datos personales se han convertido en uno de los activos más valiosos tanto para las empresas como para las instituciones públicas y privadas. La recopilación, almacenamiento y procesamiento de datos personales son actividades rutinarias que, sin la debida protección, pueden vulnerar los derechos fundamentales de las personas.

Poco se ha avanzado en determinar los beneficios de contar con una ley de protección de datos en Guatemala, ya que esto traerá múltiples beneficios a todos los niveles de la sociedad como el fortalecimiento de la confianza, seguridad jurídica, protección de derechos fundamentales, impulso a la innovación y competitividad, prevención de abusos y fraudes, transparencia y responsabilidad garantizando los derechos individuales de los ciudadanos de la República de Guatemala.

La presente iniciativa de ley representa un antecedente positivo y específico para la protección de datos personales de los ciudadanos, elaborada con el objeto de protegerlos de diversos riesgos y vulnerabilidades que implica el manejo de sus datos personales.

Es por ello, que, en ausencia de un marco regulatorio específico, se considera que la presente iniciativa de ley busca establecer un marco normativo que regule de manera efectiva el tratamiento de datos personales, garantizando la privacidad, la seguridad y la confianza de los individuos, y promoviendo el desarrollo y la competitividad digital en Guatemala y la región centroamericana. Por lo tanto, se deja en la responsabilidad de los señores Diputados, la presente iniciativa de ley, para que después de su estudio y análisis correspondiente, se apruebe como Ley de la República.

**Diputado (s) Ponente (s):**



**DIPUTADO JORGE MARIO VILLAGRÁN ÁLVAREZ**  
**CONGRESO DE LA REPÚBLICA DE GUATEMALA**

**DECRETO NÚMERO \_\_\_\_-2024**

**CONGRESO DE LA REPÚBLICA DE GUATEMALA**

**CONSIDERANDO:**

Que la Constitución Política de la República de Guatemala, en el artículo 1, establece que el Estado de Guatemala se organiza para proteger a la persona y a la familia; que su fin supremo es la realización del bien común y los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar.

**CONSIDERANDO:**

Que la Corte de Constitucionalidad, en el expediente 1356-2006, ha expresado que el amparo resulta ser la acción constitucional idónea para garantizar el derecho que a toda persona asiste de acceder a su información personal recabada en bancos de datos o registros particulares u oficiales (...) o cuando esos datos sean proporcionados por personas individuales o jurídicas que prestan un servicio al público de suministros de información de personas, a fin de positivar aquellos derechos de corregir, actualizar, rectificar, suprimir o mantener en confidencialidad información o datos que tengan carácter personal, y así garantizar el adecuado goce de los derechos reconocidos en los artículos 4º, 28 y 31 de la Constitución.

**CONSIDERANDO:**

Que la recopilación, almacenamiento y procesamiento de datos personales son actividades rutinarias que, sin la debida protección, pueden vulnerar los derechos fundamentales de las personas, y que la ausencia de una normativa clara y específica sobre protección de datos ha llevado a situaciones en las que los datos personales han sido utilizados de manera indebida, sin el consentimiento de los titulares y sin las garantías necesarias para proteger su integridad y confidencialidad.

**POR TANTO:**



En ejercicio de las atribuciones que le confiere la literal a) del artículo 171 de la Constitución Política de la República de Guatemala.

**DECRETA:**

**La siguiente:**

**“LEY DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE  
DERECHOS DIGITALES”**

**CAPÍTULO I**

**DISPOSICIONES GENERALES**

**Artículo 1. Objeto.** La presente Ley tiene por objeto proteger los datos personales de los individuos y garantizar los derechos fundamentales a la privacidad y autodeterminación informativa, relacionada a las actividades de tratamiento de datos personales realizadas por entidades responsables, ya sea públicas o privadas, dentro o fuera del territorio nacional de la República de Guatemala.

**Artículo 2. Ámbito de aplicación.** La presente Ley se aplicará a todo tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales, contenidos o destinados a ser incluidos en archivos, ficheros, soportes informáticos o electrónicos, bancos, empresas o cualquier otra forma de almacenamiento de información pública o privada en custodia, depósito o administración de las entidades, públicas o privadas, que procesen datos personales de ciudadanos guatemaltecos, dentro o fuera del territorio nacional. Se regirá por lo que establece la Constitución Política de la República de Guatemala y la presente ley.

No están sujetos a las disposiciones de esta ley, los asuntos militares o diplomáticos de seguridad nacional y los datos suministrados por particulares bajo garantía de confidencialidad y las disposiciones del Decreto 57-2008 del Congreso de la República de Guatemala.

**Artículo 3. Sujetos obligados.** Es sujeto obligado de la presente ley, toda persona física o jurídica, de naturaleza pública o privada, que, por razón de su oficio, profesión, actividad comercial o institucional, opera el tratamiento de los datos personales de guatemaltecos, dentro o fuera del territorio nacional de la República de Guatemala.





**Artículo 4. Definiciones.** Para los efectos de esta Ley, se entenderá por:

- a. **Datos personales:** Cualquier información relacionada con una persona física identificada o identificable.
- b. **Datos sensibles:** Datos personales que revelen origen racial o étnico, estado de salud, información genética, creencias religiosas, opiniones políticas, preferencias sexuales, entre otros.
- c. **Encargado del tratamiento:** Persona física o jurídica, de naturaleza pública o privada, que trate datos personales por cuenta del responsable del tratamiento.
- d. **Portabilidad de datos:** Es la capacidad de mover, copiar o transferir datos fácilmente de una base de datos, almacenamiento o entorno informático a otro, y hasta qué punto los datos pueden trasladarse fácilmente entre distintos ordenadores y entornos operativos digitales.
- e. **Titular de los datos:** Persona física a la que se refieren los datos personales.
- f. **Tratamiento de datos:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recolección, registro, organización, almacenamiento, conservación, elaboración, modificación, consulta, utilización, comunicación, difusión o supresión.

**Artículo 5. Principios.** Los principios que rigen la interpretación de la presente ley son:

- a. **Licitud, lealtad y transparencia:** Los datos personales deberán ser tratados de manera lícita, leal y transparente en relación con el titular de los datos.
- b. **Limitación de la finalidad:** Los datos personales se recogerán con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- c. **Minimización de datos:** Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- d. **Exactitud:** Los datos personales serán exactos y, si fuera necesario, actualizados; se tomarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
- e. **Limitación del plazo de conservación:** Los datos personales se mantendrán de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.
- f. **Integridad y confidencialidad:** Los datos personales serán tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño




accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

- g. **Responsabilidad.** Los responsables del tratamiento y manejo de los datos deberán adoptar medidas proactivas para garantizar el cumplimiento de la normativa de protección de datos y demostrar dicho cumplimiento ante la autoridad competente.

## CAPÍTULO II

### DERECHOS DE LOS TITULARES DE DATOS

**Artículo 6. Derechos de los titulares.** Son derechos de los titulares de datos, los siguientes:

- a. **Derecho de acceso:** Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizar, rectificar y/o enmendar.
- b. **Derecho de información:** Los titulares de los datos tienen derecho a obtener del responsable del tratamiento, confirmación del tratamiento o no, de datos personales que les conciernen, así como información detallada sobre dicho tratamiento, incluidos los fines del tratamiento, las categorías de datos personales, los destinatarios o categorías de destinatarios a quienes se han comunicado o serán comunicados los datos personales, y el plazo previsto de conservación.
- c. **Derecho de rectificación:** Los titulares de los datos tienen derecho a obtener la rectificación de los datos personales inexactos que les concierne y a que se completen los datos personales incompletos, mediante una declaración adicional.
- d. **Derecho de supresión:** Los titulares de los datos tienen derecho a obtener la supresión de los datos personales que les concierne cuando estos ya no sean necesarios para los fines para los que fueron recogidos o cuando el titular retire el consentimiento en que se basa el tratamiento, el titular se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento, los datos personales hayan sido tratados ilícitamente, o los datos personales deban suprimirse para el cumplimiento de una obligación legal.
- e. **Derecho al acceso de datos personales:** Los titulares de los datos tienen derecho a recibir los datos personales, que hayan facilitado a un responsable
- 

del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin impedimentos.

- f. **Derecho de oposición y derecho a la limitación del tratamiento:** Los titulares de los datos tienen derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que les conciernen sean objeto o no de un tratamiento, incluida la elaboración de perfiles digitales.

Los titulares de los datos tienen derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:

- i. El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos.
- ii. El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- iii. El responsable ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones.
- iv. El interesado se haya opuesto al tratamiento en virtud del derecho de oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

**Artículo 7. Derechos digitales personales.** En el marco de la presente ley, se consideran derechos digitales de carácter personal, los siguientes:

- a. **Derecho a la Privacidad digital:** Toda persona tiene derecho a la privacidad en el entorno digital, incluyendo la protección de sus datos personales y la confidencialidad de sus comunicaciones.
- b. **Derecho a la seguridad de la información:** Toda persona tiene derecho a que sus datos personales sean protegidos contra accesos no autorizados, alteraciones y destrucción mediante la implementación de medidas de seguridad adecuadas.
- c. **Derecho al olvido:** Las personas tienen derecho a solicitar la eliminación de sus datos personales sin costo alguno, cuando estos ya no sean necesarios para los fines para los que fueron recogidos, cuando se haya retirado el consentimiento, o cuando se hayan tratado de manera ilícita.
- d. **Derecho a la identidad digital:** Las personas tienen derecho a controlar su identidad digital y a corregir cualquier información errónea o desactualizada que pueda afectarla.
- e. **Derecho a la transparencia en algoritmos:** Las personas tienen derecho a ser informados sobre el uso de algoritmos en decisiones automatizadas que



afecten sus derechos y libertades, incluyendo la lógica utilizada y las posibles consecuencias de dicho tratamiento.

- f. **Derecho a la no discriminación digital:** Es toda distinción, exclusión o restricción en el entorno digital basado en los datos personales, incluyendo prácticas de perfilamiento injustas o desproporcionadas que tengan por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de sus derechos digitales, sobre la base de la igualdad, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera.

### CAPÍTULO III

#### ÓRGANO RECTOR Y OBLIGACIONES DE LOS RESPONSABLES

**Artículo 8. Órgano rector.** El órgano rector de protección de datos y garantía de derechos digitales personales de Guatemala será la Dirección de Protección de Datos Personales y Garantía de Derechos Digitales, adscrita a la Secretaría de Protección de Infraestructuras Críticas, del Consejo Nacional de Infraestructuras Críticas, que será responsable de la implementación, supervisión y cumplimiento de la presente Ley. El reglamento de la presente ley determinará lo relativo a esta dirección y su funcionamiento.

**Artículo 9. Tratamiento de solicitud expresa.** Los titulares de los datos podrán ejercer sus derechos mediante solicitud expresa dirigida al responsable del tratamiento de los datos, quien deberá responder en un plazo no mayor a 30 días a partir de la recepción de la solicitud.

En caso de que el responsable del tratamiento de los datos no atienda la solicitud en el plazo establecido o la respuesta no sea satisfactoria, el titular podrá presentar una reclamación ante la autoridad de protección de datos, que será la Dirección de Protección de Datos Personales y Garantía de Derechos Digitales, que estará a cargo de la Secretaría de Protección de Infraestructuras Críticas del Consejo Nacional de Infraestructuras Críticas, que deberá proporcionar una respuesta a las solicitudes de los titulares sin dilación y, en cualquier caso, en un plazo máximo de un mes desde la recepción de la solicitud. Este plazo podrá prorrogarse únicamente por otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. Excedido el tiempo de dos meses, el reglamento determinará las sanciones por incumplimiento de solicitudes expresas.



**Artículo 10. Obtención de consentimiento.** Los responsables del tratamiento de los datos deberán obtener el consentimiento explícito en forma física o digital de los titulares de los datos antes de recoger y tratar sus datos personales, salvo en los casos previstos por la Ley.

**Artículo 11. Transparencia en la información.** Los responsables del tratamiento de los datos deberán proporcionar a los titulares de los datos, información clara y comprensible sobre los fines del tratamiento, la identidad del responsable del tratamiento, los destinatarios de los datos personales, y los derechos que les asisten.

**Artículo 12. Medidas de seguridad.** Los responsables del tratamiento de los datos deben implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de los datos personales.

**Artículo 13. Notificación de brechas de seguridad.** En caso de una brecha de seguridad, los responsables del tratamiento deberán notificar a la autoridad de protección de datos y a los titulares de los datos afectados y en un plazo máximo de 72 horas desde que tengan conocimiento de esta.

**Artículo 14. Evaluaciones de impacto.** Los responsables del tratamiento deberán realizar evaluaciones de impacto sobre la protección de datos cuando un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

**Artículo 15. Obligaciones de los responsables.** Son obligaciones de los encargados del tratamiento de datos, los siguientes:

- a. **Cumplimiento de instrucciones:** Los encargados del tratamiento de los datos sólo tratarán los datos personales conforme a las instrucciones documentadas del responsable del tratamiento.
- b. **Medidas de seguridad:** Los encargados del tratamiento de los datos deberán implementar las medidas de seguridad adecuadas para proteger los datos personales que traten.
- c. **Subcontratación:** Los encargados del tratamiento no podrán subcontratar parte o la totalidad del tratamiento de datos sin la autorización previa y por escrito del responsable del tratamiento.
- d. **Registro de actividades:** Los encargados del tratamiento deberán llevar un registro de todas las actividades de tratamiento de datos personales realizadas por cuenta del responsable del tratamiento.



- e. **Notificación de brechas de seguridad:** En caso de una brecha de seguridad, los encargados del tratamiento de los datos deberán notificar al responsable del tratamiento sin dilación indebida, y este último deberá notificar a la autoridad de protección de datos y a los titulares de los datos afectados en un plazo máximo de 72 horas desde que tengan conocimiento de esta.
- f.

## **CAPÍTULO IV**

### **TRANSFERENCIAS INTERNACIONALES DE DATOS**

**Artículo 16. Transferencias internacionales de datos.** Las transferencias internacionales de datos personales sólo podrán realizarse a países u organizaciones internacionales que ofrezcan un nivel adecuado y seguro de protección de los datos. En ausencia de dicha protección, las transferencias internacionales sólo podrán realizarse si el responsable o encargado del tratamiento de los datos ofrece garantías adecuadas, y a condición de que los titulares de los datos dispongan de derechos exigibles y de acciones legales efectivas.

Las transferencias internacionales que no cumplan con las disposiciones anteriores sólo podrán realizarse con el consentimiento explícito del titular de los datos, o cuando la transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento, o por razones de interés público. En ausencia de una decisión de adecuación, las transferencias internacionales sólo podrán realizarse si el responsable o encargado del tratamiento de los datos ofrece garantías adecuadas, y a condición de que los titulares de los datos dispongan de derechos exigibles y de acciones legales efectivas.

## **CAPÍTULO V**

### **PROTECCIÓN DE DERECHOS DIGITALES PERSONALES**

**Artículo 17. Protección de información digital.** Todas las entidades que manejen datos personales deberán implementar medidas técnicas y organizativas adecuadas para proteger la información digital contra accesos no autorizados, alteraciones, pérdidas y destrucción.



**Artículo 18. Derecho a la información.** Los titulares de datos personales tienen derecho a ser informados de manera clara y accesible sobre cómo se recopilan, utilizan, almacenan y protegen sus datos personales, tanto en entidades públicas como privadas.

**Artículo 19. Transparencia en el tratamiento.** Las entidades públicas y privadas que traten datos personales deberán proporcionar información transparente sobre los procesos de tratamiento, incluyendo la finalidad del tratamiento, las categorías de datos tratados, los destinatarios de los datos y los plazos de conservación.

**Artículo 20. Información sobre brechas de seguridad.** En caso de una brecha de seguridad que afecte los datos personales, las entidades públicas y privadas deberán informar sin dilación a los titulares afectados, detallando la naturaleza de la brecha, las posibles consecuencias y las medidas adoptadas para mitigar los efectos.

## **CAPITULO VI**

### **PORTABILIDAD Y DECISIONES AUTOMATIZADAS**

**Artículo 21. Facilitación de la portabilidad.** Las entidades deberán facilitar la portabilidad de los datos cuando sea técnicamente posible, asegurando la interoperabilidad y la seguridad de los datos durante la transmisión.

**Artículo 22. Prohibición de decisiones automatizadas.** Los titulares de datos tienen derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzcan efectos jurídicos en ellos o les afecten significativamente de manera similar.

**Artículo 23. Intervención humana.** En los casos en que se utilicen sistemas automatizados para la toma de decisiones digitales, los titulares de datos tienen derecho a obtener exclusivamente intervención humana para expresar su punto de vista, impugnar la decisión y obtener respuesta efectiva con la intervención de personas humanas en todo el proceso.

**Artículo 24. Protección de la integridad.** Las entidades deberán garantizar la integridad de los datos personales y su exactitud, cuando sea necesario, actualizarlos adoptarán todas las medidas razonables para asegurar la corrección de los datos inexactos.



**Artículo 25. Confidencialidad de los datos.** Las entidades deberán asegurar la confidencialidad de los datos personales, implementando medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados y divulgaciones no autorizadas.

## CAPÍTULO VII

### RESPONSABILIDAD Y RENDICIÓN DE CUENTAS

**Artículo 26. Responsabilidad.** Todas las entidades que traten datos personales serán responsables del cumplimiento de las disposiciones de esta Ley y deberán demostrar dicho cumplimiento ante la autoridad competente de protección de datos, cuando así se les requiera.

**Artículo 27. Registros de actividades y tratamiento.** Las entidades deberán llevar un registro de todas las actividades de tratamiento de datos personales, incluyendo las finalidades del tratamiento, las categorías de datos tratados, los destinatarios de los datos, tomando en cuenta el uso que le dan y las medidas de seguridad adoptadas.

**Artículo 28. Educación.** El órgano rector deberá llevar a cabo campañas de educación y sensibilización para informar a los ciudadanos sobre sus derechos en materia de protección de datos personales y sobre las obligaciones de las entidades que tratan datos personales.

Las entidades públicas y privadas deberán implementar programas de formación continua para su personal, a fin de garantizar el cumplimiento de las disposiciones de esta Ley y la adecuada protección de los datos personales.

**Artículo 29. Cooperación internacional.** El órgano rector podrá cooperar con autoridades de protección de datos de otros países para asegurar el cumplimiento de esta Ley y la protección de los datos personales en contextos transfronterizos, únicamente cuando estén involucrados en temas relacionados a ciberseguridad y cibercrimen.

**Artículo 30. Transferencias internacionales seguras.** Las transferencias internacionales de datos personales deberán realizarse de acuerdo con las disposiciones de esta Ley y las garantías adecuadas para proteger los derechos de los titulares de los datos.





**Artículo 31. Protección de información digital:** Todas las entidades públicas y privadas que manejen datos personales deberán implementar medidas técnicas y organizativas adecuadas para proteger la información digital contra accesos no autorizados, alteraciones, pérdidas y destrucción. Además, deberá contar con la autorización del propietario para que puedan hacer uso de su información.

**Artículo 32. Destino.** Los recursos económicos recaudados por multas se trasladarán a los fondos privativos de la Dirección de Protección de Datos Personales y Derechos Digitales, para garantizar su adecuado funcionamiento.

## CAPÍTULO VIII

### SANCIONES, INCUMPLIMIENTO Y RECLAMACIONES

**Artículo 33. Acceso indebido.** Comete el delito de acceso indebido, quien, estando autorizado para tratar datos personales con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia, por tal hecho se le impondrán de 6 a 8 años de prisión y una multa de Q. 50,000.00 quetzales.

**Artículo 34. Lucro ilegal.** Comete el delito de lucro ilegal, quien, con el fin de alcanzar un lucro, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada, y los transmita sin su consentimiento para obtener para sí ganancias económicas. Por tal hecho se le impondrán de 6 a 8 años de prisión y una multa de Q. 50,000 quetzales.

Las sanciones de este capítulo se aplicarán sin perjuicio de las responsabilidades civiles y administrativas correspondientes y los daños y perjuicios que correspondan.

**Artículo 35. Incumplimiento.** El incumplimiento de las disposiciones de esta Ley para el caso del sector público o privado podrán dar lugar a la imposición de sanciones penales, civiles y administrativas, las cuales se regularán en el reglamento de la presente ley, sin perjuicio de los delitos cometidos, en cuyo caso corresponde a la autoridad responsable a denunciar y a los titulares de los datos recurrir ante las instancias competentes.

**Artículo 36. Reclamaciones.** Los titulares de datos personales afectados por el mal uso de su información digital tendrán derecho a presentar reclamaciones ante la autoridad de protección de datos y a recibir reparaciones por los daños y



perjuicios sufridos. También podrá acudir ante la Dirección de Atención y Asistencia al Consumidor -DIACO- para que dentro de su competencia se restablezcan sus derechos, quedando libre la vía civil o penal para el reclamo efectivo de los daños y perjuicios ocasionados por la entidad responsable.

El reglamento de la presente ley determinará lo concerniente a las reclamaciones y reparaciones que procedan.

## **CAPÍTULO IX**

### **DISPOSICIONES FINALES**

**Artículo 37. Implementación y reglamentación.** Corresponde al Organismo Ejecutivo a través de todas sus dependencias competentes, dictar las normas reglamentarias necesarias para la aplicación de esta Ley, en un plazo no mayor a seis meses a partir de su publicación en el Diario Oficial.

**Artículo 38. Vigencia.** El presente Decreto entrará en vigencia ocho días después de su publicación en el Diario Oficial.

**REMITASE AL ORGANISMO EJECUTIVO PARA SU SANCIÓN, PROMULGACIÓN Y PUBLICACIÓN.**

**EMITIDO EN EL PALACIO DEL ORGANISMO LEGISLATIVO, EN LA CIUDAD DE GUATEMALA, EL \_\_\_\_\_ DE \_\_\_\_\_ DEL AÑO DOS MIL \_\_\_\_\_.**

