



REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR



Trámite **254848**
Codigo validación **2FQYD4HAAQ**
Tipo de documento OFICIO
Fecha recepción 12-jul-2016 18:14
Numeración documento pan-gr-2016-1692
Fecha oficio 12-jul-2016
Remitente RIVADENEIRA BURBANO
GABRIELA ALEJANDRA
Función PRESIDENTA
remitente

Revise el estado de su trámite en:
<http://tramites.asambleanacional.gob.ec/estadoTramite.jsf>

Oficio No. PAN-GR-2016-1692

Quito, 12 de julio de 2016

Señora Doctora

Rosana Alvarado

PRIMERA VICEPRESIDENTA DE LA ASAMBLEA NACIONAL

En su despacho.-

De mi consideración:

De conformidad con la Ley Orgánica de la Función Legislativa, publicada en el Registro Oficial Nro. 63 de 10 de noviembre de 2009, artículo 54 numeral 1), que establece que la iniciativa para presentar los proyectos de ley corresponde a los asambleístas con el apoyo de una bancada legislativa o de al menos el cinco por ciento de sus miembros, me permito presentar, en calidad de asambleísta nacional, el Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales.

Este Proyecto cuenta con el respaldo necesario para el tratamiento en el Pleno de la Asamblea Nacional.

Atentamente,

Gabriela Rivadeneira Burbano

PRESIDENTA DE LA ASAMBLEA NACIONAL



EXPOSICIÓN DE MOTIVOS

En el contexto de la era informacional, cada día se registran millones de datos bajo distintos procedimientos. Estos se gestionan y se encuentran expuestos al público. A pesar de la existencia de una normativa internacional y nacional dirigida a la protección de la privacidad e intimidad de las personas, los riesgos surgidos del desarrollo y la expansión de las nuevas tecnologías de la información y la comunicación elevan la vulnerabilidad de las personas en el tratamiento de su información personal. Por lo tanto, se impone la necesidad de una regulación del uso público y privado de la información personal y un proceso de concienciación de la colectividad sobre la misma.

La mayoría de las actividades sociales demandan un intercambio de información y su debida sistematización: abrir una cuenta en el banco, participar en un concurso, reservar un vuelo o un hotel, efectuar un pago con tarjeta de crédito o navegar en internet. Basta con *googlear* el nombre de una persona para tener acceso a los datos sobre su estado civil, cuenta telefónica, el objeto de su negocio u otro aspecto de su vida personal. Nombres y apellidos; fecha de nacimiento; dirección domiciliaria o de correo electrónico; número de identificación; matrícula del auto y muchos otros datos que se usan a diario, constituyen información que podría permitir identificar a una persona, ya sea directa o indirectamente. Estos datos que dicen mucho sobre nosotros, nuestra vida y nuestra intimidad personal están expuestos al libre acceso; carecen de protección y pueden ser utilizados para múltiples fines, no siempre lícitos.

El entorno digital es dinámico y es necesario responder con ritmo similar y con adaptación al ordenamiento jurídico para alcanzar que, en este contexto, los derechos de los individuos sean protegidos y garantizados y por lo tanto no se vean afectados. Si bien es cierto, la Constitución de 2008 garantiza el derecho a la intimidad personal y familiar (artículo 66), en la práctica, se ha vuelto relativamente simple acceder a la información personal, que solo debería ser proporcionada por el titular.

Ante la existencia de bases de datos públicas y privadas a través de las cuales se comercializa y difunde información personal, es indispensable una ley que ampare la decisión de las personas sobre sus datos y proteger su privacidad e intimidad, tanto en la esfera de su vida individual como familiar, dando especial relevancia a los derechos de los más vulnerables: niñas, niños y adolescentes.

Los datos personales, como se ha señalado anteriormente, dicen todo sobre la vida privada e íntima de la persona y pueden revelar la identidad, en consecuencia, deben ser protegidos. El libre acceso a la información puede vulnerar derechos e incidir negativamente en el bienestar, seguridad personal y familiar y por esto, la necesidad de regular la captación, aprovechamiento y flujo de la información personal.



La Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales que se propone, da repuesta a la problemática ocasionada en el tratamiento de datos personales en una era en la que los medios tecnológicos para su procesamiento y almacenamiento se desarrollan constantemente. Esta Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales apela al derecho fundamental que tienen las personas para disponer y decidir sobre toda la información relativa a su privacidad e intimidad.

La protección de datos para que sea integral, debe actuar en dos sentidos: por un lado, establecer los derechos del titular, como son otorgar y revocar el consentimiento del uso de su información personal, actualizarla y rectificarla; y, por otro, establecer las regulaciones en el procesamiento y tratamiento de la información personal por parte de entidades públicas y privadas cuya finalidad sea exclusivamente financiera o mercantil.

Esta Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales surge sobre la base del principio de autonomía de la persona, mediante la cual se establece un marco de regulación para la administración y gestión de los datos personales.

LA ASAMBLEA NACIONAL

EL PLENO

CONSIDERANDO

Que el artículo 12 de la Declaración Universal de los Derechos Humanos dispone que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”;

Que el artículo 17 numeral 1 del Pacto Internacional de Derechos Civiles y Políticos establece que “nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y reputación; y, su numeral 2 determina que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”;

Que el artículo 11 numeral 2 de la Convención Interamericana sobre Derechos Humanos determina que “nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; y su numeral 3, sostiene que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”;



Que el artículo 66 numeral 3 de la Constitución de la República, garantiza el derecho a la integridad personal que incluye la integridad física, psíquica, moral y sexual;

Que el artículo 66 numeral 19 de la Norma Suprema “garantiza el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter, así como la correspondiente protección”;

Que el artículo 66 numeral 20 de la Norma Suprema “garantiza el derecho a la intimidad personal y familiar”;

Que el artículo 6 de la Ley Orgánica de Garantías Constitucionales y Control Constitucional dispone que “las garantías jurisdiccionales tienen como finalidad la protección eficaz e inmediata de los derechos reconocidos en la Constitución y en los instrumentos internacionales de derechos humanos, la declaración de la violación de uno o varios derechos, así como la reparación integral de los daños causados por su violación”;

Que el artículo 2 literal d) de la Ley Orgánica de Transparencia y Acceso a la Información Pública “garantiza la protección de la información personal en poder del sector público y/o privado”;

Que el artículo 78 de la Ley Orgánica de Comunicación establece que “para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20, de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal”;

Que el artículo 53 del Código de la Niñez y Adolescencia dispone que “sin perjuicio de la natural vigilancia de los padres y maestros, los niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la ley. Se prohíbe las injerencias arbitrarias o ilegales en su vida privada”;

Que el artículo 4 de la Ley del Sistema Nacional de Registro de Datos Públicos dispone que “las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo”;

Que el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos manifiesta que “son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales”;



Que el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos “determina que para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de estos, quien podrá seleccionar la información a compartirse con terceros”;

Que el artículo 178 del Código Orgánico Integral Penal tipifica el delito de violación a la intimidad y determina que “la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años”;

Que el artículo 229 del Código Orgánico Integral Penal tipifica el delito de revelación ilegal de base de datos y determina que “la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años”; y,

Que el artículo 475 numeral 1 del Código Orgánico Integral Penal establece que “la correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código”.

Por lo expuesto, la Asamblea Nacional, en ejercicio de sus atribuciones constitucionales y legales, expide la siguiente:

LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES

TÍTULO I

GENERALIDADES

Artículo 1.- Objeto. La presente Ley tiene por objeto proteger y garantizar el derecho de todas las personas a la intimidad y privacidad en el tratamiento de datos personales que se encuentren en bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas.

Artículo 2.- Ámbito de aplicación. Los principios y disposiciones contenidas en la presente Ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, en todo el territorio nacional.

Las limitaciones a los principios y derechos previstos en esta Ley, en cuanto a su observancia y ejercicio, corresponderán a la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Artículo 3.- Principios generales. Todos los involucrados en la formación, administración y manejo de bases o bancos de datos, ficheros, archivos, en forma física y/o digital, o que tengan relación con datos personales de terceros, están obligados a observar y respetar los siguientes principios:

1. **Legalidad:** la formación de bases de datos será lícita cuando se encuentren debidamente inscrita y la información haya sido obtenida por medios legítimos, en estricta observancia a la normativa en el ámbito relativo a esta materia.
2. **Pertinencia:** los datos personales no podrán ser utilizados para fines distintos a los que motivaron su obtención.
3. **Veracidad:** la recolección de datos personales deberá ser veraz y no excesiva; no podrá obtenerse por medios fraudulentos, abusivos o en forma contraria a la presente Ley.
4. **Consentimiento informado:** el titular de los datos deberá prestar su consentimiento libre, expreso, previo e informado para la entrega de los mismos. Se exceptúan los datos que provengan de fuentes públicas de información; se recaben para el ejercicio de funciones propias de las instituciones del Estado; deriven de relaciones contractuales, científicas o profesionales del titular de los datos y sean necesarias para su cumplimiento; y, se realicen por personas naturales para su uso exclusivo personal o doméstico.
5. **Confidencialidad:** tanto el responsable como el usuario de bases de datos debe adoptar medidas para resguardar de manera confidencial los datos personales, con el objeto de evitar su adulteración, pérdida o tratamiento no autorizado. Adicionalmente, los datos deberán ser almacenados de forma que permitan el acceso al titular.
6. **Reserva:** las personas naturales o jurídicas que obtengan legítimamente información proveniente de una base de datos están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de sus actividades, siendo prohibida la difusión a terceros.

Artículo 4.- Definiciones. Para los efectos de la presente Ley se entiende por:

1. **Base o banco de datos:** conjunto organizado de datos personales que es objeto de tratamiento o procesamiento, digital o no, cualquiera que sea la modalidad de su formación, almacenamiento, organización o acceso.



2. **Consentimiento del titular:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular autoriza el tratamiento de datos personales.
3. **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular.
4. **Datos sensibles:** datos que se refieren a las características físicas de la persona que revelan el origen racial y étnico, las convicciones ideológicas, filosóficas o morales, las opiniones políticas, creencias religiosas, los datos genéticos, la información referente a la salud y a la vida sexual o cualquier otro dato vinculado con la intimidad del titular.
5. **Disociación de datos:** procedimiento mediante el cual los datos personales no puedan vincularse a una persona determinada o determinable.
6. **Protección de datos personales:** facultad que otorga la Ley para que el dueño de los datos personales, decida a quién proporciona su información, cómo y para qué. Este derecho permite acceder, rectificar, cancelar y oponerse al tratamiento de su información personal.
7. **Responsable del tratamiento de la información:** persona natural o jurídica, pública o privada que sola o conjuntamente con otros, administra el sistema de tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos. Toda operación de información que comprometa datos personales, en procedimiento mecánico o automatizado que tenga como fin la recolección, ordenamiento, conservación, almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad.
8. **Responsable del archivo, registro, base o banco de datos:** persona natural o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos como custodio y operador de la información.
9. **Titular de los datos:** persona natural cuyos datos personales son objeto de tratamiento.
10. **Tratamiento de datos:** cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos en cualquier otra forma.
11. **Usuario de datos:** persona natural o jurídica, pública o privada, que realiza el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.



Artículo 5.- Tratamiento de datos sensibles. Se prohíbe el tratamiento de datos sensibles en todo aquello que pueda afectar el derecho a la intimidad de la persona. Nadie podrá ser obligado a proporcionar datos sensibles, salvo las siguientes circunstancias:

1. El titular autoriza expresamente y por escrito el tratamiento de datos sensibles.
2. El tratamiento es necesario para salvaguardar el interés vital del titular si este se encuentra física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
3. El tratamiento se refiere a datos que son indispensables para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. El tratamiento tiene una finalidad estadística, científica o académica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

TÍTULO II

DERECHOS Y OBLIGACIONES EN LA PROTECCIÓN DE DATOS

Artículo 6.- Derechos de los Titulares. El titular de los datos personales tendrá los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados del tratamiento.
2. Ser informado por el responsable o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
3. Acceder en forma gratuita a sus datos personales que han sido objeto de tratamiento en instancias públicas y privadas.
4. Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando exista orden de autoridad competente.
5. Revocar el consentimiento, oponerse y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, previo el trámite legal pertinente.
6. Presentar reclamos por incumplimiento a lo dispuesto en la presente Ley.

Artículo 7.- Derechos de las niñas, niños y adolescentes. Se asegurará el respeto al derecho a la intimidad de las niñas, niños y adolescentes, por lo que se prohíbe el



tratamiento de sus datos personales, salvo aquellos datos que sean de naturaleza pública. Es deber del Estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes respecto del tratamiento indebido de sus datos personales; y, proveer de conocimiento acerca del uso responsable y seguro por parte de niñas, niños y adolescentes de sus datos personales, su derecho a la intimidad y protección de su información personal y a la de los demás.

Artículo 8.- Obligaciones del responsable del tratamiento de la información. Constituyen obligaciones del responsable del tratamiento de la información, las siguientes:

1. Requerir y obtener el consentimiento del titular de los datos personales, previo a su obtención y tratamiento.
2. Informar al titular de los datos, en forma expresa y clara, previamente a recabar información referida a su persona, acerca de:
 - a) La existencia del archivo, registro, base o banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
 - b) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o categorías de destinatarios.
 - c) El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean formuladas.
 - d) Las consecuencias que se deriven por proporcionar los datos, por la negativa a hacerlo o por la inexactitud de los mismos.
 - e) La facultad y modo de ejercer los derechos de acceso, rectificación, actualización y supresión de los datos que le confiere la presente Ley.
3. Respetar en todo momento los principios generales de la protección de datos personales.
4. Proceder en forma inmediata a la rectificación, actualización o supresión, de los datos personales cuando fueran total o parcialmente inexactos, incompletos o desactualizados.
5. Inscribir sus archivos, registros, bases o bancos de datos en el Registro Nacional de Bases de Datos creado por el organismo de control.

Artículo 9.- Obligaciones del responsable de las bases o bancos de datos, ficheros, archivos. Le corresponde al responsable de las bases o bancos de datos, ficheros o archivos cumplir con las mismas obligaciones exigidas al responsable del tratamiento de la información tanto respecto de la confidencialidad y reserva que debe mantener sobre la



información obtenida, como del respeto y cumplimiento de los principios generales de la protección de datos personales.

El encargado de las bases de datos solo actuará según las instrucciones del responsable del tratamiento de datos y no podrá, bajo ningún concepto, ceder los datos personales sometidos a tratamiento, ni aun para su conservación.

Artículo 10.- Obligaciones del usuario de datos. Todas las personas que actúen, trabajen, o presten servicios de cualquier tipo en o para algún órgano del sector público o privado, solo podrán tratar los datos personales incorporados en las bases o bancos de datos, ficheros, archivos, de titularidad del órgano para o en el que desempeñen su tarea, cuando así lo disponga el responsable del tratamiento de la información en virtud de una obligación legal.

Quedan sujetos, al igual que los encargados del tratamiento, a los mismos deberes y obligaciones exigidos al responsable de las bases o bancos de datos, ficheros, archivos, tanto respecto de la confidencialidad y reserva que debe mantener sobre la información obtenida, como del respeto y cumplimiento a los principios generales de la protección de datos personales.

El usuario de datos solo podrá ceder los datos personales sometidos a tratamiento siguiendo expresas instrucciones del responsable del tratamiento.

TÍTULO III

TUTELA DE DERECHOS

Artículo 11.- Autoridad Nacional de Protección de Datos Personales. La Dirección Nacional de Registro de Datos Públicos adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información será la Autoridad Nacional de Protección de Datos Personales y ejercerá la vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley.

Artículo 12.- Atribuciones de la Autoridad Nacional de Protección de Datos Personales. Además de las atribuciones señaladas en otros cuerpos legales, la Dirección Nacional de Registro de Datos Públicos ejercerá las siguientes:

1. Velar por el cumplimiento de la legislación en materia de protección de datos personales.
2. Promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales e implementar mecanismos de difusión acerca del ejercicio y garantía del derecho constitucional de la protección de datos.



3. Disponer el bloqueo temporal o definitivo de los sistemas de información cuando exista un riesgo cierto de afectación de derechos constitucionales, en caso de incurrir en infracciones contempladas en esta ley.
4. Solicitar a los responsables del tratamiento y responsables de las bases o bancos de datos, ficheros, archivos, la información necesaria para el ejercicio efectivo de sus funciones.
5. Realizar las declaraciones sobre las transferencias internacionales de datos, ejercer el control y adoptar las autorizaciones que procedan en relación con estas transferencias y cooperar en materia de protección internacional de datos personales.
6. Implementar un sistema de resguardo de la información para evitar su deterioro o desaparición.
7. Crear un Registro Nacional de Bases de Datos Personales y emitir las órdenes y los actos necesarios para su administración y funcionamiento.
8. Determinar la responsabilidad de las infracciones e imponer las sanciones a los responsables del tratamiento y responsables de las bases o bancos de datos, ficheros y archivos, previo el debido proceso correspondiente.
9. Realizar la vigilancia y control de las bases o bancos de datos, ficheros o archivos físicas o digitales.
10. Realizar campañas de concientización a la población sobre la necesidad de protección de datos personales y sensibles.
11. Las demás que le sean designadas por ley.

Artículo 13.- Tutela de los derechos. Las actuaciones contrarias a lo dispuesto en la presente ley serán objeto de acción constitucional de *habeas data*, conforme con lo establecido en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

TÍTULO IV

REGISTRO NACIONAL DE BASES DE DATOS PERSONALES

Artículo 14.- Definición. El Registro Nacional de Bases de Datos Personales es el conjunto organizado de bases o bancos de datos, ficheros, archivos, en forma física o digital, de instancias públicas o privadas, que operan en el país, sujetos a tratamiento.

Artículo 15.- Administración. El Registro será administrado por la Autoridad Nacional de Protección de Datos Personales.

Artículo 16.- Inscripción registral. Todas las base o bancos de datos, ficheros o archivos, en forma física o digital, de instancias públicas y las base o bancos de datos, ficheros, o archivos, en forma física o digital de empresas e instituciones privadas con fines exclusivamente financieros y mercantiles deberán inscribirse en el Registro Nacional de



Bases de Datos Personales de acuerdo con los procedimientos y criterios que la Dirección Nacional de Registro de Datos Públicos establezca para el efecto

Artículo 17.- Tratamiento de datos efectuado por terceros. Si el responsable de archivo, registro, base de datos debe encargar a un tercero este servicio, requerirá de autorización expresa de la autoridad competente para que se realice el respectivo control.

Artículo 18.- Requisitos para la inscripción. Las bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas, para su inscripción en el Registro Nacional de Bases de Datos, deberán contener:

1. Identificación de la base de datos y el responsable de la misma.
2. Naturaleza de los datos que contiene.
3. Procedimientos de obtención y tratamientos de los datos.
4. Medidas de seguridad y descripción técnica de la base de datos.
5. Declaración sobre la protección de datos personales.
6. Destino de los datos y personas físicas o jurídicas a las que puedan ser transmitidos.
7. Tiempo de conservación de los datos.
8. Forma y condiciones en que las personas pueden acceder a los datos.
9. Procedimientos para la rectificación o actualización de los datos.

El incumplimiento de estos requisitos dará lugar a la sanción prevista en esta Ley.

Artículo 19.- Autorización de Operaciones. Las bases o bancos de datos, ficheros, archivos, en forma física o digital provenientes del sector privado, para ejecutar sus actividades, además de la inscripción obligatoria en el Registro Nacional de Bases de Datos contarán con una autorización de operaciones.

La Autoridad Nacional de Protección de Datos Personales establecerá mediante reglamento los requisitos y procedimientos para la obtención de la autorización.

TÍTULO V

TRANSFERENCIA INTERNACIONAL DE DATOS

Artículo 20.- Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países u organismos internacionales que no proporcionen niveles de protección de datos, conforme con las normas de derecho internacional o regional en la materia.

Artículo 21.- Excepciones. La prohibición a la que se refiere el artículo anterior no será de aplicación en los siguientes casos:



1. Cuando el titular haya otorgado su autorización expresa e inequívoca para la transferencia de datos personales.
2. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico.
3. Cuando se refiera a transferencias bancarias o bursátiles, conforme con la legislación aplicable.
4. Cuando la transferencia internacional de datos resulte de la aplicación de tratados o convenios internacionales en los cuales Ecuador sea parte, con fundamento en el principio de reciprocidad.
5. Cuando la transferencia sea necesaria o legalmente exigida para salvaguardar el interés público.
6. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
7. Cuando 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 siempre y cuando se cuente con la autorización del titular.

TÍTULO VI

INFRACCIONES Y SANCIONES

Artículo 22.- Responsabilidad. Sin perjuicio de incurrir en infracciones penales, en caso de incumplimiento con lo previsto sobre la protección de datos personales, los responsables de tratamiento, los responsables de las bases o bancos de datos, ficheros, archivos, en forma física o digital y los usuarios, en instancias públicas y privadas, estarán sujetos al régimen sancionatorio, conforme con el presente Título.

Artículo 23.- Clasificación de las infracciones. Según su magnitud e importancia, las infracciones se clasifican en leves y graves.

Artículo 24.- Infracciones leves. Son las siguientes:

1. No inscribir el banco de datos en el Registro Nacional de Bases de Datos.
2. Proceder a recoger datos de carácter personal sin proporcionar la debida información conforme con lo establecido en el artículo 8, numeral 2, de esta Ley.
3. Mantener datos de carácter personal inexactos, pese la solicitud de rectificación de los mismos.
4. Mal manejo administrativo del archivo y tratamiento de bases de datos.

Artículo 25.- Infracciones graves. Se determinan como infracciones graves las siguientes:

1. Recoger datos en forma engañosa o fraudulenta.
2. Recabar y tratar datos sensibles, sin consentimiento expreso del titular y no guardar la respectiva confidencialidad.

3. Crear bases o bancos de datos, ficheros y archivos con datos sensibles.
4. No atender la solicitud del titular de los datos o de la Autoridad Nacional de Protección de Datos Personales sobre la supresión, rectificación y actualización de los datos personales cuando legalmente proceda.
5. Realizar transferencia temporal o definitiva de datos de carácter personal hacia el extranjero, que hayan sido recogidos u objeto de tratamiento, con destino a organismos gubernamentales, organismos internacionales, ONG, empresas transnacionales públicas y privadas y cualquier otra entidad que no proporcionen ningún nivel de protección, de acuerdo con las normas regionales o internacionales correspondientes.
6. Obstruir las funciones que por esta Ley se le reconoce a la Autoridad Nacional de Protección de Datos.
7. Tratar los datos de carácter personal de un modo que lesione, violente o desconozca los derechos a la intimidad, imagen, identidad y honor, así como cualquier otro derecho de que sean titulares las personas naturales.
8. Obstruir las funciones de vigilancia y control de la Autoridad Nacional de Protección de Datos.
9. Crear bases o bancos de datos, ficheros, archivos, en forma física o digital sobre datos personales sin el cumplimiento de los requisitos establecidos en esta Ley.
10. Iniciar el tratamiento de los datos de carácter personal o usarlos conculcando principios y garantías determinadas en la Constitución y en esta Ley.
11. No guardar la debida confidencialidad sobre los datos de carácter personal incorporados a bases o bancos de datos, ficheros y archivos.
12. Reincidir en cualquier infracción leve.

Artículo 26.- Sanciones. Las sanciones que se impondrán a causa del cometimiento de las infracciones señaladas en los artículos precedentes serán:

1. Amonestación por escrito.
2. Multa de uno a diez salarios básicos unificados.
3. Inmovilización de las bases o bancos de datos, ficheros o archivos.
4. Retiro temporal de las bases o bancos de datos, ficheros o archivos.
5. Retiro definitivo de las bases o bancos de datos, ficheros o archivos.

Artículo 27.- Graduación de las sanciones. Las sanciones se graduarán según los siguientes lineamientos:

1. Valoración de derechos constitucionales afectados.
2. Volumen de los tratamientos efectuados.
3. Beneficios económicos obtenidos.
4. Grado de intencionalidad.
5. Reincidencia en la comisión de la infracción.
6. Daños y perjuicios causados a titulares o terceras personas.



7. Reconocimiento o aceptación expresa sobre la infracción investigada, antes de la imposición de la sanción.

Artículo 28.- Procedimiento. La Autoridad Nacional de Protección de Datos Personales determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación con la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

La máxima autoridad del Ministerio de Telecomunicaciones y Sociedad de la Información será quien resuelva en última y definitiva instancia los recursos que se presenten.

En caso de verificarse la posible existencia de infracción penal, la Autoridad Nacional de Protección de Datos Personales comunicará a las autoridades penales correspondientes para su debida investigación.

DISPOSICIÓN REFORMATORIA

ÚNICA.- Añádase a continuación del numeral 1 del artículo 31 de la Ley del Sistema Nacional de Registro de Datos Públicos el siguiente numeral:

“1.1 Ejercer las funciones como Autoridad Nacional de Protección de Datos Personales conforme a lo dispuesto en la Ley de Protección de Datos Personales.”

DISPOSICIÓN TRANSITORIA

PRIMERA.- La Autoridad Nacional de Protección de Datos Personales deberá crear el Registro Nacional de Bases de Datos en el plazo máximo de ciento ochenta días a partir de la publicación de la presente Ley.

SEGUNDA.- Para la aplicación de la presente Ley, se dictará el correspondiente Reglamento en el plazo de 90 días.

DISPOSICIÓN FINAL

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Suscrito en Quito, Distrito Metropolitano, a los



REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

**FIRMAS DE RESPALDO AL PROYECTO DE LEY ORGÁNICA DE
PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD
SOBRE LOS DATOS PERSONALES**

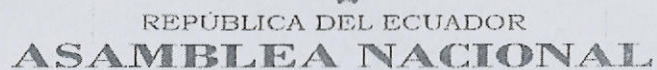
NOMBRE	FIRMA
Andrés Moya	
Hólgan Chávez C.	
ÁNGEL RIVERA	
Alberto Zambrano	
RENE CAZA	
G. Pivora López	
ALBERTO ARIAS	
GILBERTO GUAMANBATE	
Diana Moreno	



REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

**FIRMAS DE RESPALDO AL PROYECTO DE LEY ORGÁNICA DE
PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD
SOBRE LOS DATOS PERSONALES**

NOMBRE	FIRMA
Mauricio Proano	
Oscar Iguacua	
Carlos Viteri	
Marilyn Uscón	
Dora A. Aguirre Hidalgo	
Raúl Abad Velaz	
Rosa Elvira Muñoz	
Betty Jerez	
Raúl Tobar Núñez	

[illegible]