

## **EXPOSICIÓN DE MOTIVOS LEY DE ACCESO, INTEGRIDAD Y PROTECCIÓN DEL DATO.**

En la República Bolivariana de Venezuela con la promulgación de la Ley Sobre Mensajes de Datos y Firmas Electrónicas en el Año 2001, se estableció el marco conceptual y de derecho para el reconocimiento de las transacciones electrónicas, tarifando el valor legal de las mismas y las consecuencias erga omnes derivadas de las transacciones o actos generados en formato electrónico y a través de la Internet.

El uso de tecnología de la información se constituye hoy día en herramienta fundamental en la gestión pública y privadas de organizaciones y entidades de gobierno, las cuales a través de redes nacionales e internacionales mantienen intercambios de todo tipo, incluyendo el comercial a través de la transferencia de informaciones de un computador a otro sin necesidad de utilizar documentos escritos en papel, lo que permite ahorro de tiempo y dinero.

El Decreto de Ley Sobre Mensajes de Datos y Firmas Electrónicas, contempló el uso de firmas electrónicas y otorgó una definición preliminar acerca del concepto de “Mensaje de Dato”.

La firma electrónica permite al usuario identificarse en internet; garantizar la autoría, la integridad del mensaje y establecer el no repudio de la transacción o de los mensajes electrónicos que haya generado un usuario en particular. Mediante el uso de la firma electrónica, el usuario se encuentra en capacidad de firmar correos y documento electrónicos en varios formatos, lo cual ofrece la oportunidad de maximizar las gestiones de instancias públicas y privadas, cimentando entre otros, los elementos constitutivos del gobierno electrónico y comercio electrónico.

El “Mensaje de Dato” creado e intercambiado con firma o certificado electrónicos a tenor de lo hasta ahora expuesto, reviste de plena prueba respecto de su contenido y de su origen, lo cual permite ofrecer mayores niveles de aseguramiento de las transacciones, aportando mejores mecanismos de control que propendan a una mayor economía, seguridad y transparencia de las transacciones electrónicas en general.

Bajo este mismo principio, la Ley de Mensajes de Datos y Firmas Electrónicas definió como “Mensaje de Dato” lo siguiente *“Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio”*.

El tratamiento asignado al dato bajo los presupuestos del Decreto de Ley Sobre Mensajes de Datos y Firmas Electrónicas, establecen una definición amplia y no especializada del dato como elemento constitutivo de valor económico y

legal en el escenario actual de las transacciones electrónicas.

Las bases de datos de instituciones públicas y privadas poseen información de usuarios y de gobierno; dicha información reviste diferentes usos y debe ser tramitada conforme al uso para el cual fue requerida, contemplando limitaciones para funcionarios públicos o empleados de empresas donde el Estado tenga participación mayoritaria o empresas privadas, respecto al acceso a dichos archivos, manejo de la información calificada como sensible y estableciendo una garantía para el usuario, en relación al conocimiento debido del uso de su dato personal por parte de las distintas instancias de gobiernos o empresas privadas, otorgando la garantía de restricción de uso, cuando así sea solicitado por el usuario interesado y que posea legitimación para actuar.

Punto adicional y de necesaria referencia dentro del contenido del presente proyecto de Ley de Acceso, Integridad y Protección del Dato, lo constituye la referencia a la aplicación de las mejores prácticas y estándares a los fines de resguardar y garantizar la recuperación ante desastres, que genere la pérdida de la información contenida en la base de datos de entidades públicas o privadas. Lo anterior se hace imperante a los fines de prevenir pérdidas de información, como las generadas en el incendio ocurrido en octubre de 2004 y que afectó al Sistema del SETRA del Instituto Nacional de Tránsito y Transporte Terrestre; lo cual derivó en pérdida de información confidencial, clasificada y de registros de datos que afectaron al colectivo en general y a la imagen del mencionado Instituto, al crear incertidumbre jurídica sobre temas tan delicados como la titularidad, propiedad o registros del parque automotor existente dentro de la República Bolivariana de Venezuela.

Como consecuencia de lo expuesto, se hace necesaria e inminente la regulación de las distintas modalidades del Dato y su tratamiento en los procesos de intercambio de información por medios electrónicos, a los fines de garantizar un marco jurídico indispensable que permita a los diversos actores involucrados del sector público o privado, desarrollarse y contribuir con el avance de las nuevas tecnologías dentro de la República Bolivariana de Venezuela.

El trato no ajustado del uso de dato se encuentra contemplado en el presente proyecto de Ley de Acceso, Integridad y Protección del Dato, estableciendo los supuestos de ley y sanciones contenidos de la Ley N° 48. Ley Especial Contra los Delitos Informáticos, publicada en la Gaceta Oficial de la República de Venezuela N° 37.313 de fecha 30 de octubre de 2001 y en el decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicada en la Gaceta Oficial de la República de Venezuela N° 37.148 de fecha 28 de febrero de 2001.

Entre los principios que guían el presente proyecto de Ley de Acceso, Integridad y Protección del Dato, destacamos los siguientes:

1. El presente proyecto de Ley de Acceso, Integridad y Protección del Dato es el

de desarrollar el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 21, referido al Derecho de Igualdad ante la Ley, garantizando a través de las acciones de los legitimados legales, la contraloría social de las entidades de gobiernos o entidades privadas a los fines de prevenir actos discriminatorios fundados en la raza, sexo, credo, condición social u orientación política.

2. A través del control y resguardo del cumplimiento del principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 21, se ofrece igualmente garantía de cumplimiento del artículo 20 ejusdem a los fines de establecer el Derecho al Libre Desarrollo de la Personalidad como derecho humano y garantía inalienable consagrada en el texto constitucional.
3. Desarrolla igualmente el Proyecto de Ley de Acceso, Integridad, y Protección del Dato, el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 28, referido al Derecho y Acción de Habeas Data, garantizando en todo momento el acceso al dato personal del interesado o colectivo interesado a los fines de poder conocer el trato asignado a sus datos personales y poder ejercer de forma oportuna las acciones o recursos que consideren necesarios, amparados bajo el marco legal.
4. Igualmente se contempla en las previsiones del proyecto de Ley, el desarrollar el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 44, numeral 2, referido a los Registros de Detenidos y al debido trámite que debe ser asignado a los mismos por entes públicos o privados; a los fines de prevenir menoscabo o lesiones en los derechos constitucionales individuales de las personas que figuren en dichos registros.
5. Se establece una garantía fundamental y de obligatoria atención por parte del Estado, la cual es la de desarrollar el principio consagrado en la Constitución de la República Bolivariana de Venezuela en sus artículos 51 y 58, referidos al Derecho de Petición y Respuesta y Derecho a la Información Oportuna, respectivamente, garantizando el debido trámite y oportuna evacuación de consultas o peticiones, lo cual redundará en garantía del cumplimiento del principio constitucional contenido en el artículo 49 que está referido al Derecho al Debido Proceso.
6. Se constituye en el proyecto de Ley un principio garantista de los Derechos Humanos que se contempla en la Constitución de la República Bolivariana de Venezuela en su artículo 56, Parágrafo Primero, referido al Derecho a Identidad y Registro sin calificaciones de ningún tipo
7. Igualmente trata el Proyecto de Ley lo referido al principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 60, referido al Derecho al Honor y Privacidad; previniendo el uso no autorizado

de información sensible y dato personal de un individuo sin contar con su autorización expresa y por escrito.

8. Se contempla igualmente en el Proyecto de Ley propuesto, las responsabilidades derivadas por el uso no ajustado del dato, ya sea por deficiencias en los procesos de protección electrónica del mismo o por la facilitación de acceso de dicho dato por parte de terceros no autorizados a tales fines.
9. La adecuación del marco normativo reposa en las mejores prácticas internacionales y nacionales en materia de seguridad de la información, ello en virtud de volumen de información que hoy día es procesada y almacenada en medios electrónicos por entidades públicas o privadas. Adicionalmente, el ente rector se encuentra creado y en operación, estando bien delimitadas sus atribuciones por el marco legal vigente en la República Bolivariana de Venezuela; todo lo cual permitirá la aplicación de la Ley sin que ello requiera de cambios en el marco legal o adecuaciones tecnológicas de gran impacto financiero y técnico que pudieran limitar la aplicación del texto normativo hoy propuesto.
10. Un aspecto relevante del Proyecto de Ley es el trato establecido a la definición de Dato, como un elemento estratégico y de valor para las organizaciones públicas o privadas que hacen vida dentro de la República Bolivariana de Venezuela. De esta manera, con la aplicación del texto normativo propuesto, se garantizará la continuidad de las operaciones y actividades de entes públicos o privados que sufran eventos de seguridad o siniestros que afecten sus registros electrónicos o informáticos y en consecuencia puedan causar lesiones o daños legales o patrimoniales a terceras personas, cuyos derechos y registros en formato electrónico que se vea afectado o destruido.

Como elemento de necesaria referencia, se señala que el impacto económico generado con la implantación del presente Proyecto de Ley de Acceso, Integridad y Protección del Dato sobre las instituciones públicas o privadas en bajo, dado que el estándar sobre el cual se encuentran generados los certificados electrónicos y que permitirá la firma de los mensajes de datos, documentos electrónicos en todas sus extensiones, es el Protocolo X-509 V3.

El mencionado protocolo ha sido considerado por estándar internacional impuesto a los desarrolladores de software licenciado y abierto a los fines de la operación conforme de los referidos softwares; igualmente los fabricantes de hardware a nivel mundial tienen considerado el Protocolo mencionado y a tales fines han dispuestos de repositorios de certificados electrónicos dentro de los sistemas operativos existentes en el mercado posteriores al año 2003. Adicionalmente, los mensajes que sean firmados electrónicamente no requieren para su trámite que los destinatarios posean certificados electrónicos para permitir su lectura o uso.

En virtud de las consideraciones que preceden, se propone el presente Proyecto de Ley, el cual queda contenido en los términos siguientes:

## **LEY DE ACCESO, INTEGRIDAD Y PROTECCIÓN DEL DATO**

### **Título I**

### **Ley de Protección del Dato**

### **Capítulo I**

### **Disposiciones Generales**

#### **Artículo 1 – Objeto**

La presente ley reviste carácter de orden público y es creada a los fines de establecer garantía de cumplimiento, disponibilidad, integridad, protección y resguardo del dato en cumplimiento del mandato impuesto en los artículos 28 y 51 de la Constitución de la República Bolivariana de Venezuela, referidos al acceso a la información en fuentes públicas o privadas y derecho a solicitar y recibir respuesta por parte de entes públicos; así como regular el tratamiento ajustado a derecho, legítimo y controlado de los datos personales o de interés público que se encuentran asentados en archivos, registros, base de datos o cualesquiera otros medios técnicos de procesamiento o almacenamiento de datos en entes públicos o privados y a los efectos de garantizar la privacidad personal y el derecho al libre ejercicio de los derechos individuales y grupales de las personas naturales o jurídicas dentro de la República Bolivariana de Venezuela.

#### **Artículo 2 - Ámbito de Aplicación**

El ámbito de aplicación de la presente ley se extiende a todos los datos registrados o almacenados en bases de datos, sean estas administradas por entidades u organizaciones de naturaleza pública o privada.

Parágrafo Primero: No obstante lo previsto en la presente ley, las bases de datos cuyo contenido haya sido declarado como “Confidencial” o “Secreto” por parte de los órganos de Inteligencia del Estado Venezolano o por las Fuerzas Armadas de la República Bolivariana de Venezuela y exclusivamente con el fin de poder garantizar la seguridad nacional interna y externa de la nación, se le aplicará el período de reserva de acceso a la información señalando en el artículo 3, numeral 3.7 del presente texto normativo.

#### **Artículo 3 - Definiciones.**

Con el objeto de ofrecer una interpretación adecuada al sentido y alcance de la presente ley, a continuación, se enunciarán una serie de conceptos, cuyas denominaciones en plural o singular atenderán al significado que se asigna a continuación:

- 3.1. Base de Datos: Significa el conjunto de Datos indistintamente su naturaleza, que se encuentran almacenados y designan al conjunto organizado de datos personales que sean objeto de tratamiento o

procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- 3.2. Custodio de Base de Datos: Significa la organización o entidad pública gubernamental centralizada o no, forma societaria mercantil o civil, que a los fines de desarrollar el mandato que le es impuesto por Ley o cumplir o desarrollar su objeto social, deban captar a través de cualquier medio datos personales o sensibles de individuos y mantenerlos en bases de datos de su exclusiva propiedad.
- 3.3. Dato: Significa el hecho o hechos, conjunto de información numérica o alfanumérica o reseña de fuente oficial, gubernamental o privada que guardan relación con personas naturales o jurídicas, obtenidos con el consentimiento del individuo que la genera y que pueden ser almacenados o registrados en medios digitales, electrónicos, físicos o informáticos.
- 3.4. Dato de Libre Acceso: Significa el dato que bajo mandato y reserva de ley debe ser del dominio o manejo público, sin mayor limitación que las establecidas por la Constitución y las leyes.
- 3.5. Dato Personal: Significa todo dato relacionado y asociado directamente con una persona natural o jurídica, pública o privada y que comporte información de índole particular y exclusiva del individuo, considerándose como tal, la información asociada a registro civil, antecedentes penales, información y registros académicos, administrativos ante entes de gobierno centralizados o no, comercial, financiera, judicial, laboral y tributaria.
- 3.6. Dato Sensible: Significa el dato personal que permita establecer o determinar la condición médica, sanitaria, biomédica, genoma del individuo, origen racial, étnico, orientación ideológica, política, religiosa o sexual, participación en movimientos de defensa de los derechos humanos, derechos laborales y de defensa de los derechos de las minorías.
- 3.7. Dato con Reserva Gubernamental de Acceso: Significa todo dato relacionado y asociado directa o indirectamente con órganos del alto gobierno que incluye la Presidencia y Vicepresidencia de la República, carteras ministeriales y órganos subordinados a dichas carteras, el Ministerio Público, la Procuraduría de la Nación y los entes y organismos del estado cuyo objeto sea la seguridad y defensa y que formen parte de la administración pública, centralizada o no, y cuyo acceso se encuentre limitado por razones de defensa nacional, seguridad interna y de índole geoestratégico. En todo caso, el dato con reserva gubernamental de acceso se regulará por el mandato impuesto en la Constitución, respecto al acceso a la información y fuente oficial,

estableciendo como plazo máximo para acceder a dicha información el de cinco (5) años contados a partir de la fecha de creación del dato o información que se trate. Individuo: Significa la persona natural o jurídica dueña de la información y de la cual emanan los datos personales.

- 3.8. Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio y que sea generada por personas naturales, jurídicas o medios automatizados digitales, informáticos o telemáticos de origen público o privado.
- 3.9. Uso No Autorizado del Dato: Significa el uso del dato no ajustado a las autorizaciones dadas por el Individuo al momento de suministrar dicho Dato.
- 3.10. Usuario de Datos: Significa la organización o entidad pública gubernamental centralizada o no, forma societaria mercantil o civil, pública o privada, que a los fines de desarrollar el mandato que le es impuesto por ley o cumplir o desarrollar su objeto social, deban utilizar los Datos de individuos usuarios de sus sistemas, a los fines de atender toda clase de recursos, acciones o solicitudes, ejecutar operaciones de cualquier índole, tramitar providencias o notificaciones de cualquier índole y que guarden relación con el usuario solicitante ante el sistema de que se trate.
- 3.11. Usuario de Sistemas: Significa el individuo que previa autorización permite la utilización de sus datos personales y sensibles por parte de una organización o entidad pública gubernamental centralizada o no, forma societaria mercantil o civil, pública o privada y con el fin de obtener respuesta a sus trámites o solicitudes de cualquier índole y sujeto a las restricciones que puedan imponer la Constitución y las leyes. El usuario de sistemas que labore o guarde cualquier tipo de dependencia con una organización o entidad pública gubernamental centralizada o no, forma societaria mercantil o civil, pública o privada y que utilice los datos de otros Individuos tendrá la doble condición de usuario y custodio de base de datos y en consecuencia asumirá las consecuencias que la ley impongan ante el uso no autorizado del dato.
- 3.12. Reserva de Base de Datos: Significa la obligación de los custodios de bases de datos de mantener sistemas o mecanismos de protección o resguardo suficientes, idóneos y legales de las bases de datos bajo su custodia y con el fin de prevenir cualquier tipo de uso, modificación, cambio o supresión no autorizado.

## **Capítulo II** **Marco de Aplicación**

### **Artículo 4 - Trámites ante Entes de Gobierno.**

Se constituye en obligación de orden público impuesto a usuarios de datos y

usuarios de sistemas, el garantizar el debido almacenamiento, resguardo y protección del dato a los fines de garantizar la integridad, el acceso, la recuperación ante desastres, el no repudio y la validez legal del dato.

#### **Artículo 5 - Acceso al Dato y a la Información.**

Se establece el principio de libre acceso al dato y la información contenida en bases de datos públicas o privadas, portales web públicos o privados y archivos públicos y privados. La libertad de acceso se encontrará directamente relacionada con el interés legítimo y directo del usuario y sujeto a las limitaciones impuestas por la Constitución y leyes especiales.

#### **Artículo 6 - Protección del Dato.**

Se constituye en obligación de orden público de aquel usuario de datos y usuario de sistemas, el de solicitar y obtener la autorización de uso del dato correspondiente, debidamente firmada por el Individuo propietario del dato ya sea de forma manual o mediante firma electrónica generada conforme a la Ley Sobre Mensajes de Datos y Firmas Electrónicas. Todo uso de dato sensible debe corresponder con actividades lícitas y debidamente autorizadas por la más alta representación de usuarios de datos y usuarios de sistemas, o por vía judicial, en cumplimiento de lo establecido en el presente cuerpo normativo, la Constitución y las leyes.

Parágrafo Primero: No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique por la más alta representación de usuarios de datos y usuarios de sistemas, la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines específicos que persigue el sujeto regulado y que son fijados por el presente cuerpo normativo, la Constitución y las leyes.

La omisión en el cumplimiento del debido trámite de la autorización contemplada en el presente aparte dará lugar a la obligación de denuncia pública obligatoria ante los órganos auxiliares y de administración de justicia. Toda transferencia de dato por parte de usuario de Dato y/o Usuario de Sistema deberá ser justificada y contar con la aprobación del responsable de reserva de base de datos, sean estos públicos o privados, señalando a tales fines motivo que genera la transferencia de dato en cualquiera de las definiciones contenidas en la presente ley.

#### **Artículo 7 - Principios Rectores Referidos al Dato.**

El uso, administración resguardo, protección y destrucción se encuentra asociado a principios rectores de obligatorio cumplimiento, los cuales se indican a continuación:

- 7.1. Principio de fidelidad y veracidad del dato. Se constituye en la obligación de orden público de aquel usuario de datos y usuario de sistemas de mantener registros fieles a la identidad del Individuo propietario del dato

y que ofrezcan información verdadera, completa, exacta, actualizada, comprobable, comprensible y asequible por medios informáticos y telemáticos con las autorizaciones correspondientes. Igualmente se constituye en obligación de orden público de aquel usuario de datos y usuario de sistemas el mantener y ofrecer datos completos, quedando totalmente prohibido el almacenamiento de datos de forma parcial, incompleta, no ajustada a la fidelidad de su origen, parciales o que permitan inducir a error o usurpación de identidad. Los usuarios de sistemas deberán acreditar su identidad a través del uso de firma electrónica emitida por un Proveedor de Servicios de Certificación (PSC) debidamente acreditado ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio de Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela, conforme a lo establecido en la Ley Sobre Mensajes de Datos y Firmas Electrónicas, su Reglamento y norma administrativa que regula la materia emanada de la mencionada superintendencia.

- 7.2. Principio de Uso Limitado. Se constituye en la limitación de orden público impuesta a usuarios de datos y usuarios de sistemas, de utilizar información de datos personales o sensibles de individuos sin otros fines que los estrictamente asociados al trámite o de solicitudes en marcha y relacionadas con la actividad de que desarrolla el usuario de dato y/o usuario de sistemas, garantizando en todo momento la confidencialidad, protección y seguridad de dicho dato a los fines de prevenir el acceso o uso no autorizado aun cuando el dato por el paso del tiempo deje de servir para el fin por el cual fue suministrado.
- 7.3. Principio de Legalidad. Significa que el uso del dato por parte del usuario de dato y usuario de sistema, debe corresponderse con fines lícitos y sujeto a las restricciones impuestas por la Constitución y las leyes; con el fin de garantizar el derecho de hábeas data, el derecho al buen nombre y la reputación, el derecho a la intimidad y el derecho a la información.

#### **Artículo 8 - Resguardo de Datos.**

Se constituye en obligación de orden público impuesto a usuario de dato y usuario de sistema, el de garantizar el debido almacenamiento, resguardo y protección del dato a los fines de garantizar la integridad, el acceso, la recuperación ante desastres, el no repudio y la validez legal del dato.

Parágrafo Primero: El debido almacenamiento, resguardo y protección del dato a los fines de garantizar la integridad, el acceso, la recuperación ante desastres, el no repudio y la validez legal del dato; se encuentran sujetas al cumplimiento de los principios contenidos en la Ley Sobre Mensajes de Datos y Firmas Electrónicas, su Reglamento y las mejores prácticas reconocidas internacionalmente en materia de seguridad de la información establecidas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio de Ciencia, Tecnología e Innovación de

la República Bolivariana de Venezuela.

El incumplimiento del mandato impuesto en el presente artículo dará lugar a la aplicación de las sanciones impuestas en el presente cuerpo normativo y de las formas legales que coincidan con las tipificaciones previstas en la Ley Contra Delitos Informáticos.

#### **Artículo 9 - Transferencia internacional.**

Está prohibida la transferencia del dato personal, dato sensible y dato con reserva a cualquier país u organismos internacionales o supranacionales, que no garanticen de forma cierta y razonable, el cumplimiento de un estándar de seguridad que proporcione niveles adecuados de protección, resguardo y uso del dato solicitado. La prohibición contemplada en el presente artículo no aplicará en los casos siguientes:

- 9.1. Colaboración judicial internacional;
- 9.2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica y motivado a un proceso de cambio, alteración o usurpación de identidad que genere conflictos o problemas con la identificación de los sujetos afectados;
- 9.3. Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;
- 9.4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Bolivariana de Venezuela sea parte;
- 9.5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

#### **Artículo 10 - Obligación de Suministro de Datos**

Se constituye en obligación de orden público para todo usuario de dato y usuario de sistemas de suministrar a los individuos bajo la definición de la presente ley, la información correspondiente al dato personal del solicitante, cuando el mismo figure en el registro de la base de datos de la entidad o se presuma su existencia. En tal sentido el Individuo en ejercicio legítimo de su derecho constitucional al buen nombre, a la no discriminación y trato igualitario y a la privacidad, ejercerá los derechos y garantías que se indican a continuación:

- 10.1. Podrá solicitar información a los organismos de control ciudadano y de policía, relativa a la existencia de archivos, registros, bases de datos donde figuren sus datos personales y conocer las finalidades con las cuales se utiliza o utilizó dicho dato personal; así como conocer de forma precisa la identidad de las personas responsables de manejar dicha información

personal. Todo usuario de dato y usuario de sistema se encuentra en la obligación de mantener un registro que permita validar los datos personales de los interesados, previa identificación y acreditación; dicho registro será público, gratuito y contará con la alternativa de consulta en línea previa identificación del Individuo con su certificado electrónico de identidad.

- 10.2. El individuo titular de dato personal, previa acreditación de su identidad, tiene derecho a solicitar y obtener de forma gratuita información de sus datos personales incluidos en las bases de datos públicas o privadas destinadas a la prestación de servicios bancarios, financieros y asegurador. Todo usuario de dato y usuario de Sistema se encuentra en la obligación de mantener un registro que permita validar el dato personal de los interesados, previa identificación y acreditación; dicho registro será público, gratuito y contará con la alternativa de consulta en línea previa identificación del Individuo con su certificado electrónico de identidad.
- 10.3. El individuo titular de dato personal, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de su dato personal incluido en las bases de datos públicas o privadas destinadas a la prestación de los servicios de consumo masivo, telefonía, certificación electrónica, entretenimiento, mercadeo, publicidad, ventas programadas y médicos, con excepción del secreto médico que se establece por reserva de Ley. Todo usuario de dato y usuario de Sistema se encuentra en la obligación de mantener un registro que permita validar el dato personal del interesado, previa identificación y acreditación; dicho registro será público, gratuito y contará con la alternativa de consulta en línea previa identificación del Individuo con su certificado electrónico de identidad.
- 10.4. Todo Individuo tiene derecho a que sea rectificado, actualizado y, cuando corresponda, suprimido o sometido a confidencialidad su dato personal, cuando este se encuentre incluido en una base de datos propiedad de un usuario de datos y/o usuario de Sistema. Todo usuario de datos y usuario de sistema se encuentra en la obligación de mantener un registro que permita validar el dato personal del interesado, previa identificación y acreditación; dicho registro será público, gratuito y contará con la alternativa de consulta en línea previa identificación del individuo con su certificado electrónico de identidad.

Parágrafo Primero: La solicitud de información contemplada en el presente artículo podrá ser efectuada mediante solicitud escrita presentada por el interesado, consulta electrónica previa autenticación con certificado electrónico de identidad o mediante solicitud firmada electrónicamente por el interesado y enviada a la dirección electrónica que debe mantener todo usuario de datos y/o usuario de sistemas, a los fines de poder tramitar las solicitudes en línea del

individuo interesado.

### **Artículo 11 - Trámite de la consulta de Dato.**

Se constituye en obligación de orden público para todo usuario de dato y usuario de sistema, el suministrar y ejecutar a solicitud de un individuo bajo la definición de la presente ley, la información y/o cambios correspondientes al dato personal del solicitante cumpliendo para ello condiciones siguientes:

- 11.1. Proporcionar la información solicitada por escrito dentro de los veinte (20) días siguientes a la fecha de recepción de la solicitud. La consulta en línea debe mantenerse disponible, garantizando la seguridad de la comunicación de intrusos o manipulaciones por parte de terceros; dicho aseguramiento será a través del uso de certificados electrónicos de seguridad, los cuales deberán encontrarse dentro de la Raíz de Certificación Nacional.
- 11.2. Proceder a la rectificación, supresión o actualización del dato personal del individuo solicitante, realizando la operación necesaria a tales fines en el plazo máximo de veinte (20) días calendario, contados a partir de la fecha de la solicitud escrita o por vía electrónica según sea el caso.
- 11.3. Cuando la base de dato sea manejada por cuenta de terceros, éstos deberán contar con la debida autorización por parte del propietario del dato personal e igualmente se encuentran obligados a ejecutar las solicitudes de los individuos cuyo dato personal se encuentre almacenado en la base de datos que corresponda, estableciéndose que dicho dato personal no podrá ser utilizado con un fin distinto al autorizado en el contrato de servicios correspondiente, ni ser cedido, modificado o copiado una vez sea procesado originalmente o transferido a otras personas o entes públicos y/o privados de forma alguna, ni aun para su conservación, quedando obligados los terceros prestadores del servicio a destruir el dato del individuo que se trate de la base de datos, una vez finalice la relación con el usuario de datos y usuario de sistemas, debiendo suministrar a tales fines constancia escrita que establezca la destrucción del dato que se trate.
- 11.4. Las entidades que ejecuten intermediación financiera, servicios bancarios, corretaje de bolsa o intercambio de valores, sólo podrán tratar dato persona de carácter patrimonial relativo a la solvencia económica, crédito o dato personal del sujeto que ejecute cualquier tipo de trámite ante dichas entidades, bajo la premisa que dicho dato personal es obtenido de fuentes accesible al público o procedente de información facilitada por el interesado propietario del dato personal, requiriendo en todo momento la autorización expresa y por escrito con el consentimiento de propietario de dato personal que se trate. Queda a criterio y potestad del propietario del dato personal, el autorizar a la entidad que ejecute la intermediación

financiera, servicio bancario, corretaje de bolsa o intercambio de valores, para utilizar dicho dato personal con fines distintos al de la transacción o actividad para la cual fue suministrado. No se permitirá el uso por parte de las entidades que ejecuten intermediación financiera, servicios bancarios, corretaje de bolsa o intercambio de valores, con fines distintos a los que generaron la solicitud de dicho dato y los que establezca la Ley.

**Título II**  
**Capítulo I**  
**Órganos De Control**

**Artículo 12 - Órgano Rector.**

Se constituye a la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela, como el ente de gobierno encargado de informar, monitorear y fiscalizar el contenido y cumplimiento de la presente Ley.

Parágrafo Primero: La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) será el ente gubernamental encargado de aplicar las sanciones administrativas contempladas en la presente ley, en los casos de incumplimiento por parte de todo usuario de dato y usuario de sistemas, público o privado y de instruir los expedientes contentivos de dichas infracciones que deben ser enviadas a los órganos de administración de justicia y defensoría del pueblo, cuando el caso contemple delitos o violaciones a los derechos humanos contenido en el marco legal aplicable dentro de la República Bolivariana de Venezuela.

A los fines de garantizar y establecer el alcance y aplicación de la presente ley, en relación con las mejores prácticas para la protección y acceso al dato por parte de todo usuario de dato y usuario de sistemas, público o privado, se crea la Certificación de Administración Conforme del Dato, cuyas características, condiciones y requisitos serán reglamentados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación.

**Artículo 13 - Instrucción de Acciones por parte del Órgano Rector.**

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación, será la encargada de sustanciar administrativamente todas las acciones o denuncias que le sean informadas y presentadas por los individuos afectados por infracciones al cuerpo normativo contenido de la presente ley. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), se encuentra en la obligación de sustanciar y dar trámite oportuno a las denuncias que reciba acerca de incumplimiento de la presente ley, oficiando lo conducente al Ministerio Público y a la Defensoría del Pueblo de la República Bolivariana de

Venezuela.

Parágrafo Primero: El Ministerio Público valiéndose del concurso de sus funcionarios y de los órganos auxiliares y de administración de justicia, instruirá las acciones que le sean remitidas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación en materia de incumplimiento de la presente Ley. De igual manera procederá la Defensoría del Pueblo, cuando sea notificada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), acerca de incumplimiento de la presente ley.

#### **Artículo 14 - Facultades del Órgano Rector.**

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela, como ente de gobierno encargado de informar, monitorear y fiscalizar el contenido y cumplimiento de la presente ley, queda facultado a realizar las acciones siguientes:

- 14.1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley.
- 14.2. Asistir y asesorar a todo propietario de dato, usuario de dato y/o usuario de sistemas que así lo requieran, acerca del alcance de la presente ley y de los medios legales de que disponen para la defensa y cumplimiento de los derechos y deberes que ésta garantiza e impone;
- 14.3. Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;
- 14.4. Realizar un censo del dato contenido o almacenado por usuarios de datos y usuarios de sistemas, públicos o privados, que presten servicios a terceros de carácter gubernamental, servicios masivos, financieros, bancarios, entretenimiento y comercial. Las personas naturales deberán acatar el cumplimiento de la presente ley, respecto al manejo del dato en todas sus acepciones bajo las definiciones contenidas en el presente texto normativo.
- 14.5. Controlar la observancia de las normas sobre integridad y seguridad del dato por parte de los usuarios de datos y usuarios de sistemas, públicos o privados, que presten servicios a terceros de carácter gubernamental, servicios masivos, financieros y bancarios, entretenimiento y comercial. A tal efecto, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), deberá garantizar el cumplimiento de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, en lo referido a la garantía de la validez, integridad, disponibilidad ulterior del dato, no repudio y autoría

del mensaje de dato por parte de los usuarios de datos y usuarios de sistemas;

- 14.6. Solicitar información a los usuarios de datos y usuarios de sistemas, públicos o privados, que presten servicios a terceros de carácter gubernamental, servicios masivos, financieros y bancarios, entretenimiento y comercial; acerca de los elementos, mecanismos y sistemas de seguridad y control de acceso al dato que manejen en sus bases de datos y portales web, a los fines de garantizar la integridad, confidencialidad y seguridad del dato aportado y almacenado por los usuarios de datos y usuarios de sistemas, en sus correspondientes bases de datos.
- 14.7. Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y del reglamento que se dicte;
- 14.8. Constituirse en querellante en las acciones penales que sean promovidas por violaciones a la presente ley;
- 14.9. Emitir la Certificación de Administración Conforme del Dato, por parte de los usuarios de datos y usuarios de sistemas usuarios, ajustándolas a las mejores prácticas de seguridad de información y recuperación ante desastres.
- 14.10. Controlar el cumplimiento de los requisitos y garantías que deben reunir los usuarios de datos y usuarios de sistemas en sus bases de datos, para obtener la correspondiente certificación de administración conforme del dato creada por la presente ley.
- 14.11. El órgano de control gozará de autonomía funcional.

## **Capítulo II** **Sanciones**

### **Artículo 15. - Entes sancionadores.**

La imposición de las sanciones derivadas del incumplimiento de la presente ley será asignada a la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), de conformidad con lo establecido en el 12 que precede. Todo procedimiento asociado a denuncias por incumplimiento de la presente ley, será ventilado ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), quien deberá oficiar al Ministerio Público y la Defensoría del Pueblo, a los fines de informar acerca de la apertura y sustanciación de las referidas denuncias.

Parágrafo Primero: En caso de omisión culposa o dolosa por parte de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE); el Ministerio Público y la Defensoría del Pueblo coordinadamente procederán de

oficio ante las instancias administrativas y judiciales que les corresponda, a los fines de salvaguardar y garantizar el derecho de los denunciantes legitimados. El lapso contemplado para dar respuesta por parte de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), a los denunciantes legitimados, acerca de los hechos denunciados es de veinte (20) días a tenor de lo dispuesto en la Ley Orgánica de Procedimiento Administrativo, siendo imperante la simplificación de trámites administrativos a tenor de lo establecido en la Ley de Simplificación de Trámite Administrativo.

#### **Artículo 16 - Monto de las sanciones.**

Sin perjuicio de las responsabilidades administrativas, civiles y penales que correspondan a todo usuario de dato y usuario de Sistema, público o privado, derivado de proceso administrativo firme y producto de la inobservancia de la presente ley, el organismo de rector impondrá multas que oscilan entre Trescientas Unidades Tributarias (300 U.T.) y Quinientas Unidades Tributarias (500 U.T.). Las sanciones serán impuestas de forma concurrente a los responsables en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias o atenuantes existentes.

Parágrafo Primero: El Reglamento de la presente Ley determinará las condiciones y procedimientos para la aplicación de las sanciones aquí previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando en todo momento el debido proceso.

#### **Artículo 17 - Sujetos Susceptibles de Sanción.**

Serán sujetos de las sanciones contempladas en la presente Ley y de forma conexa las contempladas en la Ley de Delitos Informáticos, todos los directores y accionistas de las personas jurídicas, públicas o privadas, los gerentes de informática o tecnología de la información y personal encargado de administrar la custodia y seguridad del dato en todas sus acepciones y definiciones contenidas en el artículo 1 de la presente ley.

#### **Artículo 18 - Sanción por Reincidencia.**

En caso de reincidencia en la infracción de la presente ley por parte de todo usuario de datos y usuario de sistema, público o privado, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), oficiará al Ministerio Público, convirtiéndose en querellante y aplicándose en su totalidad la sanción de multa contenida en el artículo 16 que precede. Igualmente se podrá ordenar el cierre temporal hasta por setenta y dos (72) horas de todo usuario de dato y usuario de sistema, público o privado, que preste servicio a terceros de carácter gubernamental, servicios masivos, financieros, bancarios, entretenimiento y comercial. En caso de una tercera reincidencia se podrá ordenar el cierre o cese de actividad.

**Título III**  
**Capítulo I**  
**Disposiciones Transitorias**

**Artículo 19 - Vigencia.**

La presente ley entrará en vigencia contados noventa (90) días, a partir de su fecha de publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Artículo 20 - Reglamento.**

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela, dictará el Reglamento que desarrolla la presente ley, dentro de los sesenta (60) días siguientes a la fecha de publicación del presente cuerpo normativo en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Artículo 21 - Adecuación de Órganos de Control**

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ente adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación de la República Bolivariana de Venezuela, el Ministerio Público y la Defensoría del Pueblo, adecuarán su infraestructura tecnológica a los fines de garantizar el cumplimiento de los principios contenidos en la presente ley y con el propósito de garantizar el cumplimiento de su actividad supervisora, rectora, contralora y ejecutora de los principios y garantías amparados por la presente ley. Dicha adecuación no debe exceder de un plazo de noventa (90) días siguientes a la fecha de publicación del presente cuerpo normativo en la Gaceta Oficial de la República Bolivariana de Venezuela.

## **EXPOSICIÓN DE MOTIVOS LEY CONTRA EL ACOSO VIRTUAL.**

El presente proyecto y propuesta para el establecimiento de la Ley Contra el Acoso Virtual, se constituye en un cumplimiento del mandato constitucional contenido en el artículo 60<sup>1</sup> de la Carta Fundamental, el cual deriva de la necesidad de establecer un cuerpo normativo ajustado a las necesidades y problemas existentes y referidos a las agresiones o acciones ejecutadas desde entornos virtuales, que actualmente no son mayormente procesadas por carecer de un instrumento que de forma expresa y precisa ofrezca mecanismos de protección a las personas de su fuero personal e íntimo, respecto de acciones constitutivas de Acoso Virtual ejecutadas por personas, grupo de personas o entes privados o de gobierno.

El uso de tecnología de la información y redes sociales virtuales, ha experimentado en los últimos años un crecimiento sostenido y una masificación en su uso, comprendiendo entre la comunidad de usuario distintos grupos etarios, los cuales han generados distintos tipos de dinámicas, donde de forma recurrente se observan conductas hostiles a través de la comunicación virtual, que pueden afectar o agredir la integridad psíquica y física de una determinada persona o grupo de personas, exponiéndolas a potenciales daños morales, psicológicos o físicos.

En la República Bolivariana de Venezuela, no existe un cuerpo normativo que de forma expresa y precisa trate el fenómeno del acoso virtual; comprendiendo como tal, la agresión o ataque que se constituya en una acción, tentativa de acción o amenaza de acción potencial o clara contra una persona o grupo de personas y que implique, establezca, sugiera o incite al menoscabo y/o afectación de la personalidad, daño físico o moral, exposición no autorizada de Dato Personal, desprecio público, incitación para delinquir por parte de los emisores de un mensaje virtual a través de una Red Social, Mensaje de Dato o a través del uso de una Plataforma Tecnológica Gubernamental.

De esta forma surge la obligación constitucional contenida en los artículos 19<sup>2</sup> y 20<sup>3</sup> de la Carta Fundamental, referida a la obligación del Estado Venezolano de garantizar el libre ejercicio sin menoscabo de los derechos humanos de los ciudadanos. Lo cual, a los efectos del presente proyecto de Ley, se traduce en la posibilidad de todo ciudadano indistintamente de su condición, raza, credo u orientación sexual, de expresarse libremente a través de redes sociales y medios virtuales; contando a tales fines con un marco legal que regule y contemple su protección ante actos o hechos constitutivos de Acoso Virtual.

La protección constitucional se extiende a la persona física, su psiquis y libre albedrío y es por ello que el artículo 46<sup>4</sup> Constitucional establece la obligación de crear un esquema de respeto y protección a la integridad física, psíquica y moral de los ciudadanos, garantizándose en todo momento la obligación por parte del Estado de proteger a la persona frente a los actos perturbadores y que potencialmente

---

<sup>1</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

<sup>2</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 19. El Estado garantizará a toda persona, conforme al principio de progresividad y sin discriminación alguna, el goce y ejercicio irrenunciable, indivisible e interdependiente de los derechos humanos. Su respeto y garantía son obligatorios para los órganos del Poder Público de conformidad con la Constitución, los tratados sobre derechos humanos suscritos y ratificados por la República y las leyes que los desarrollen.

<sup>3</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 20. Toda persona tiene derecho al libre desenvolvimiento de su personalidad, sin más limitaciones que las que derivan del derecho de las demás y del orden público y social.

<sup>4</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 46. Toda persona tiene derecho a que se respete su integridad física, psíquica y moral, en consecuencia: 1. Ninguna persona puede ser sometida a penas, torturas o tratos crueles, inhumanos o degradantes. Toda víctima de tortura o trato cruel, inhumano o degradante practicado o tolerado por parte de agentes del Estado, tiene derecho a la rehabilitación. 2. Toda persona privada de libertad será tratada con el respeto debido a la dignidad inherente al ser humano. 3. Ninguna persona será sometida sin su libre consentimiento a experimentos científicos, o a exámenes médicos o de laboratorio, excepto cuando se encontrare en peligro su vida o por otras circunstancias que determine la ley. 4. Todo funcionario público o funcionaria pública que, en razón de su cargo, infiera maltratos o sufrimientos físicos o mentales a cualquier persona, o que instigue o tolere este tipo de tratos, será sancionado o sancionada de acuerdo con la ley.

afecten su fuero de integridad física, psíquica y moral, tal y como lo contempla el artículo 55<sup>5</sup> de la Constitución Nacional.

La protección del Estado no debe entenderse como una violación o restricción del libre ejercicio de la opinión contemplado en el artículo 57 de la Constitución Nacional<sup>6</sup>. La Ley Contra el Acoso Virtual, se orienta precisamente a garantizar el libre desenvolvimiento y al establecimiento de quien haga uso de este derecho, asume plena responsabilidad por todo lo expresado, limitando en todo caso el anonimato o la propaganda de guerra, mensajes discriminatorios o los que promuevan la intolerancia religiosa, racial o de orientación sexual.

Todo estado moderno se fundamenta en el respecto a la diversidad de las opiniones y posiciones asumidas por un ciudadano o grupo de ciudadanos. De esta manera la censura se encuentra velada, pues se constituye en la vía expedita de descomposición del elemento democrático que debe garantizar el libre desenvolvimiento del ciudadano o grupo de ciudadano, siempre sujeto al cumplimiento del ordenamiento legal tal y como lo contempla el artículo 58<sup>7</sup> de la Carta Fundamental. La diversidad de criterios y posiciones enriquece el elemento social y propende a la formación integral y libre de las personas. Todo lo anterior se puede ver afectado por la presencia de acciones a través de redes o medios virtuales, en donde individuos de forma aislada fomenten ideas o acciones orientadas a dañar emocional o físicamente a una persona o grupo de personas.

El uso de las redes sociales no comporta la obligación de un permiso o autorización que valide la capacidad o condición física, psíquica, intelectual, moral, religiosa o racional de una persona y es precisamente allí donde radica el espíritu de la libertad y la posibilidad de expresión de ideas y conceptos, todo lo cual permite el libre desenvolvimiento y desarrollo personal. En todo caso, lo que debe ser regulado, es la acción que un sujeto o grupo de sujetos ejecute a través de un entorno virtual y solo si esa acción, a tenor del mandato constitucional contenido en el artículo 61<sup>8</sup>, es de una naturaleza tal que pueda ser considerada como un acto violento o incitador de violencia psicológica, sexual, social, política, de género, religiosa<sup>9</sup> o racial; que en definitiva es el objeto y alcance del presente proyecto de Ley.

Especial importancia a los fines del objeto y alcance de la Ley Contra Acoso Virtual, lo constituye la protección a la población de menores de edad que utilizan las redes sociales, pues en esa población se presenta con mayor presencia hechos constitutivos de conductas abusivas como el bullying, la incitación a la comisión de actos sexuales pedofilia, incitación a la prostitución y exposición no autorizada, incitación al consumo de sustancias tóxicas o psicotrópicas, las cuales una vez

---

<sup>5</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 55. Toda persona tiene derecho a la protección por parte del Estado a través de los órganos de seguridad ciudadana regulados por ley, frente a situaciones que constituyan amenaza, vulnerabilidad o riesgo para la integridad física de las personas, sus propiedades, el disfrute de sus derechos y el cumplimiento de sus deberes.

<sup>6</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 57. Toda persona tiene derecho a expresar libremente sus pensamientos, sus ideas u opiniones de viva voz, por escrito o mediante cualquier otra forma de expresión, y de hacer uso para ello de cualquier medio de comunicación y difusión, sin que pueda establecerse censura. Quien haga uso de este derecho asume plena responsabilidad por todo lo expresado. No se permite el anonimato, ni la propaganda de guerra, ni los mensajes discriminatorios, ni los que promuevan la intolerancia religiosa. Se prohíbe la censura a los funcionarios públicos o funcionarias públicas para dar cuenta de los asuntos bajo sus responsabilidades.

<sup>7</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 58. La comunicación es libre y plural, y comporta los deberes y responsabilidades que indique la ley. Toda persona tiene derecho a la información oportuna, veraz e imparcial, sin censura, de acuerdo con los principios de esta Constitución, así como el derecho de réplica y rectificación cuando se vean afectados directamente por informaciones inexactas o agraviantes. Los niños, niñas y adolescentes tienen derecho a recibir información adecuada para su desarrollo integral.

<sup>8</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 61. Toda persona tiene derecho a la libertad de conciencia y a manifestarla, salvo que su práctica afecte la personalidad o constituya delito. La objeción de conciencia no puede invocarse para eludir el cumplimiento de la ley o impedir a otros su cumplimiento o el ejercicio de sus derechos.

<sup>9</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 59. El Estado garantizará la libertad de religión y de culto. Toda persona tiene derecho a profesar su fe religiosa y cultos y a manifestar sus creencias en privado o en público, mediante la enseñanza u otras prácticas, siempre que no se opongan a la moral, a las buenas costumbres y al orden público. Se garantiza, así mismo, la independencia y la autonomía de las iglesias y confesiones religiosas, sin más limitaciones que las derivadas de esta Constitución y la ley. El padre y la madre tienen derecho a que sus hijos o hijas reciban la educación religiosa que esté de acuerdo con sus convicciones. Nadie podrá invocar creencias o disciplinas religiosas para eludir el cumplimiento de la ley ni para impedir a otro u otra el ejercicio de sus derechos.

ejecutadas afectarán el desarrollo e integridad psíquica y física del menor y de su futuro dentro de la sociedad. Es por ello por lo que en cumplimiento del mandato constitucional contenido en el artículo 78<sup>10</sup> se procede al establecimiento del presente proyecto de Ley Contra el Acoso Virtual.

Entre los principios que guían el presente proyecto de Ley Contra el Acoso Virtual, destacamos los siguientes:

1. El presente proyecto de Ley Contra Acoso Virtual cumple y desarrollo el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 60, referido al Derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación
2. A través del control y resguardo del cumplimiento del principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 20 se ofrece igualmente garantía de cumplimiento del Derecho al Libre Desenvolvimiento de la Personalidad como derecho humano y garantía inalienable consagrada en el texto constitucional.
3. Desarrolla igualmente el Proyecto de Ley Contra Acoso Virtual, el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 59, referido a la libertad de religión y de culto y poder ejercer de forma oportuna las acciones o recursos que consideren necesarios, amparados bajo el marco legal.
4. Igualmente se contempla en las previsiones del proyecto de Ley, el desarrollar el principio consagrado en la Constitución de la República Bolivariana de Venezuela en su artículo 61, referido a la libertad de conciencia y a manifestarla; a los fines de prevenir menoscabo o lesiones en los derechos constitucionales individuales de las personas, siempre en cumplimiento de las limitaciones que imponga la Ley.
5. Se establece una garantía fundamental y de obligatoria atención por parte del Estado, la cual es la protección a los menores consagrado en el artículo 78 de la Constitución de la República Bolivariana de Venezuela, a través del desarrollo del contenido de la Constitución, por medio de las previsiones contenidas en el Proyecto de Ley Contra Acoso Virtual, las cuales establecen la protección y reparación ante la ocurrencia de actos constitutivos de violencia virtual.
6. Se contempla igualmente en el Proyecto de Ley propuesto, las responsabilidades derivadas por el uso no ajustado de las comunicaciones y mensajes de datos enviados o dirigidos a través de medios virtuales en formato electrónico o a través de redes sociales privadas o comunitarias, con independencia de la territorialidad del dominio y siempre sujeto a las condiciones de uso y legislación que regulen a las redes sociales que se encuentren involucradas en un hecho que se constituya en un agresión o ataque virtual en contra de una persona natural o grupo de persona naturales.
7. La adecuación del marco normativo reposa en las mejores prácticas internacionales y nacionales en materia de seguridad de la información, ello en virtud de volumen de información que hoy día es procesada en formato electrónico o a través de redes sociales privadas o comunitarias. Adicionalmente, el ente rector se encuentra creado y en operación, estando bien delimitadas sus atribuciones por el marco legal vigente en la República

---

<sup>10</sup> Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N° 5.453 de fecha 24 de marzo de 2000. Artículo 78. Los niños, niñas y adolescentes son sujetos plenos de derecho y estarán protegidos por la legislación, órganos y tribunales especializados, los cuales respetarán, garantizarán y desarrollarán los contenidos de esta Constitución, la Convención sobre los Derechos del Niño y demás tratados internacionales que en esta materia haya suscrito y ratificado la República. El Estado, las familias y la sociedad asegurarán, con prioridad absoluta, protección integral, para lo cual se tomará en cuenta su interés superior en las decisiones y acciones que les conciernan. El Estado promoverá su incorporación progresiva a la ciudadanía activa, y un ente rector nacional dirigirá las políticas para la protección integral de los niños, niñas y adolescentes.

Bolivariana de Venezuela; todo lo cual permitirá la aplicación de la Ley sin que ello requiera de cambios en el marco legal o adecuaciones tecnológicas de gran impacto financiero y técnico que pudieran limitar la aplicación del texto normativo hoy propuesto.

Como elemento de necesaria referencia, se señala que el impacto económico generado con la implantación del presente Proyecto de Ley Contra Acoso Virtual, se refiere al establecimiento, creación y puesta en operación de la Dirección Especial contra Delitos Informáticos del Ministerio Público, estableciendo el Proyecto de Ley Contra Acoso Virtual, que mientras se cumpla con la creación de la Dirección Especial contra Delitos Informáticos del Ministerio Público; toda denuncia de acoso virtual será sustanciada y tramitada por la Dirección General de Actuación Procesal, en su Dirección de Protección de Derechos Fundamentales. Otro punto referido al impacto económico, se corresponde con el uso de certificados electrónicos generados bajo la Raíz de Certificación del Estado Venezolano, lo cual no puede ser considerado como un requisito adicional que debe ser presupuestado, dado que la Ley de Infogobierno, establece para los órganos del Estado Venezolano, el uso de dicho certificados, siendo que su procura ya debe estar contemplada en las partidas presupuestarias de los organismos públicos involucrados dentro de los procesos establecidos en el Proyecto de Ley Contra Acoso Virtual.

En virtud de las consideraciones que preceden, se propone el presente Proyecto de Ley Contra Acoso Virtual, el cual queda contenido en los términos siguientes:

## **LEY CONTRA EL ACOSO VIRTUAL**

### **Título I**

#### **Disposiciones Fundamentales**

##### **Capítulo I**

#### **Disposiciones Generales**

**Artículo 1 – Objeto:** La presente ley reviste carácter de orden público y es creada a los fines de fungir como mecanismos de protección, defensa y resguardo de la integridad psicológica, social, moral y física de personas naturales, ante agresiones o ataques recibidos a través de medios virtuales o redes sociales virtuales. Igualmente, la presente Ley contempla mecanismos de prevención administrativos y/o judiciales, a los fines de prevenir la ocurrencia o hacer cesar todo acto que se constituya en una agresión o ataques virtual en contra de una persona natural o grupo de persona naturales.

**Artículo 2 - Ámbito de Aplicación:** El ámbito de aplicación de la presenta ley se extiende a todas las comunicaciones y mensajes de datos enviados o dirigidos a través de medios virtuales en formato electrónico o a través de redes sociales privadas o comunitarias, con independencia de la territorialidad del dominio y siempre sujeto a las condiciones de uso y legislación que regulen a las redes sociales que se encuentren involucradas en un hecho que se constituya en un agresión o ataque virtual en contra de una persona natural o grupo de personas naturales.

**Artículo 3 – Definiciones:** Con el objeto de ofrecer una interpretación adecuada al sentido y alcance de la presente ley, a continuación, se enunciarán una serie de conceptos, cuyas denominaciones en plural o singular atenderán al significado que se asigna a continuación:

- 3.1. Acoso Virtual: Significa toda agresión o ataque que se constituya en una acción, tentativa de acción o amenaza de acción potencial o clara contra una persona o grupo de personas y que implique, establezca, sugiera o incite al menoscabo y/o afectación de la personalidad, daño físico o moral, exposición no autorizada de Dato Personal, desprecio público, incitación para delinquir por parte de los emisores de un mensaje virtual a través de una Red Social, Mensaje de Dato o a través del uso de una Plataforma

Tecnológica Gubernamental.

- 3.2. Conducta exhibicionista con contenido sexual explícito no autorizado: Consiste en toda forma de agresión sexual virtual, no consentida o autorizada por la víctima y que el actor perpetrador ejecute por sí o por intermedio de terceros o medios digitales.
- 3.3. Dato: Significa el hecho o hechos, conjunto de información numérica o alfanumérica o reseña de fuente oficial, gubernamental o privada que guardan relación con personas naturales o jurídicas, obtenidos con el consentimiento del individuo que la genera y que pueden ser almacenados o registrados en medios digitales, electrónicos, físicos o informáticos.
- 3.4. Dato de Libre Acceso: Significa el dato que bajo mandato y reserva de ley debe ser del dominio o manejo público, sin mayor limitación que las establecidas por la Constitución y las leyes.
- 3.5. Dato Personal: Significa todo dato relacionado y asociado directamente con una persona natural pública o privada y que comporte información de índole particular y exclusiva del individuo, considerándose como tal, la información asociada a registro civil, antecedentes penales, información y registros académicos, administrativos ante entes de gobierno centralizados o no, comercial, financiera, judicial, laboral y tributaria o cualquier otra información de índole personal reservada del conocimiento público, sin que medie previamente consentimiento expreso y escrito de la persona cuya información sea revelada.
- 3.6. Dato Sensible: Significa el dato personal que permita establecer o determinar la condición médica, sanitaria, biomédica, genoma del individuo, origen racial, étnico, orientación ideológica, política, religiosa o sexual, participación en movimientos de defensa de los derechos humanos, derechos laborales y de defensa de los derechos de las minorías.
- 3.7. Dominio Abierto Disponible: Significa todo dominio de acceso público y disponible a través de Internet y que puede ser constituido por una página web, red social, Blog o cualquier otro mecanismo o medio de interacción o socialización de personas en un ambiente virtual y por medio del uso de equipos y tecnologías de la información.
- 3.8. Plataforma Tecnológica Gubernamental: Significa toda infraestructura equipos, partes, componentes, equipos y personal de Tecnología de Información que se constituyen en una plataforma tecnología de un ente público o empresa donde el Estado Venezolano guarde participación accionaria mayoritaria o guarde participación accionaria de cualquier clase y que sea utilizado para mantener comunicación y enviar mensajes de datos a otras entidades de gobierno o particulares, se encuentre estos dentro o fuera de la República Bolivariana de Venezuela.
- 3.9. Mensajes de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio y que sea generada por personas naturales, jurídicas o medios automatizados digitales, informáticos o telemáticos de origen público o privado.
- 3.10. Red Social: Significa el sitio de Internet privado o público, con dominio abierto disponible donde la persona natural ha creado un perfil de usuario mediante el cual interactúa con distintos individuos, comunidades, emite concepto o fija posiciones y expone y sube fotografías, videos, grabaciones o imágenes de índole personal o laboral, formados por comunidades de individuos con intereses o actividades en común (como amistad, parentesco, educación o trabajo) y que permiten el contacto entre estos,

de manera que se puedan comunicar e intercambiar información.

## **Capítulo II**

### **Marco de Aplicación**

**Artículo 4 – Protección Contra Segregación:** Se constituye en obligación de orden público impuesta por Ley a usuarios de datos y usuarios de sistemas públicos o privados y redes sociales, el garantizar y prevenir toda conducta que atente, contra una persona o grupo de personas y que sea violatoria de los derechos que prevalecen a la persona humana independientemente de la condición social, religión practicada, origen étnico, inclinación política, tendencia sexual o cualquier otra condición inherente a la naturaleza humana y que sea sujeto de protección por parte de las leyes venezolanas o tratados internacionales suscritos, aceptados y en aplicación dentro de la República Bolivariana de Venezuela.

**Artículo 5 – Actos Sujetos a Control de la Ley:** Se establece el principio de presunción de buena fe, libertad de expresión y libre albedrío en las comunicaciones virtuales; no obstante, existen limitaciones establecidas en la legislación venezolana y que serán sujeto de aplicación en concurrencia a las sanciones que establezca la presente Ley, respecto a los actos que se indican a continuación:

1. Acoso Virtual escolar (bullying).
2. Acoso Virtual a menores de edad.
3. Exposición Virtual de Dato Personal sin autorización.
4. Acoso Virtual por razones políticas.
5. Acoso Virtual por razones religiosas.
6. Acoso Virtual por razones de género u orientación sexual.
7. Acoso Laboral.
8. Incitación al suicidio.
9. Conducta exhibicionista con contenido sexual explícito no autorizado.

La libertad de la comunicación virtual, cualquiera que ella sea, se encontrará directamente relacionada con el interés legítimo y directo del emisor y del destinatario del mensaje; siempre sujeto a las limitaciones impuestas por la Constitución y leyes especiales.

**Artículo 6 - Protección Ante el Acoso Virtual:** Se constituye en obligación de orden público y de obligatoria atención y trámite por parte de las instancias públicas y privadas involucradas, el prestar la debida asistencia, a las denuncias efectuadas por las víctimas o representante de las víctimas de acoso virtual que les sean presentadas. Aquellas autoridades que conozcan ya sean por denuncia o de oficio, de hechos que revistan el carácter de Acoso Virtual, deberán agotar las instancias correspondientes a los fines de garantizar la cesación del acto constitutivo de Acoso Virtual, prevenir reincidencias o daños psicológicos o físicos de los afectados por Acoso Virtual. La omisión en el cumplimiento de sus obligaciones y efectuar el debido trámite, acarreará al funcionario incurso, la aplicación de las sanciones civiles, penales y administrativas que establezca la Ley, siendo adicionalmente responsable de los daños y perjuicios que se ocasionen con motivo de la inacción o falta de trámite debido.

**Artículo 7 – Sustanciación de Expediente por Acoso Virtual:** El Ministerio Público será el órgano instructor de las denuncias sobre acoso virtual creándose a los fines de la presente ley, una Dirección Especial contra Delitos Informáticos. Mientras se cumple el mandato de la presente Ley, en el sentido de crear y colocar en operación la Dirección Especial contra Delitos Informáticos; toda denuncia de acoso virtual será sustanciada y tramitada por la Dirección General de Actuación Procesal, en su Dirección de Protección de Derechos Fundamentales. El Ministerio Público deberá en todo momento notificar a la Defensoría del Pueblo. El Ministerio Público apoyará su gestión de investigación en el Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC) y en el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela (VENCERT).

Parágrafo Primero: Efectuada la instrucción del caso dentro de los lapsos de Ley, el Ministerio Público estará en la obligación de remitir el expediente a la Jurisdicción Penal a los fines de proseguir los tramites de Ley. Todo acto del proceso seguido ante el Ministerio Público deberá ser informado vía correo electrónico firmado electrónicamente a la víctima y al presunto agravante, a los fines de ejercer su derecho a la defensa y cumplir con el debido proceso. En protección de la víctima, el Fiscal del Ministerio Público podrá solicitar la aplicación de las medidas preventivas o cautelares requeridas para la interrupción o cesación del hecho denunciado como acoso virtual.

**Artículo 8 - Resguardo de Datos y Manejo de Expediente:** El Ministerio Público, el Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC) y el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela (VENCERT) utilizarán medios electrónicos para tramitar y sustanciar expedientes, investigaciones y pruebas. Todos los archivos electrónicos que sean generados por los organismos previamente definidos en este artículo, deberán ser asegurados con certificados electrónicos generados bajo la Raíz de Certificación Venezuela, por un Proveedor de Servicios de Certificación (PSC) acreditado ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), a los fines de garantizar la integridad, no repudio y autoría de las informaciones, experticias y otros documentos electrónicos que formen parte del expediente de Acoso Virtual. El resguardo del expediente electrónico será efectuado por el Ministerio Público.

Parágrafo Primero: Los miembros del Ministerio Público, el Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC), el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela (VENCERT) y las partes, es decir la víctima denunciante, así como el presunto agraviado, que formen parte de un expediente sobre acoso virtual, deberán colocar a disposición una dirección electrónica válida que los identifique, a los fines de ser informados acerca de todas las incidencias y resultados del proceso.

**Artículo 9 – Medidas Preventivas o cautelares:** En fase de instrucción el Ministerio Público podrá tomar fundamentando en la Ley, las medidas que considere necesarias para instruir el expediente, prevenir la comisión de un hecho ilícito o la continuidad del acto constitutivo del Acoso Virtual. El juez de instancia que conozca acerca de la denuncia de Acoso Virtual deberá considerar las medidas preventivas o cautelares solicitadas por el Ministerio Público o por la víctima; estableciendo si el caso lo amerita las medidas preventivas complementarias que considere necesarias, procedan por Ley y sean necesarias para la cesación del acto constitutivo de Acoso Virtual.

## **Título II**

### **Capítulo I**

#### **Medidas Remediadoras**

**Artículo 10 – Para la Víctima:** Toda Víctima de Acoso Virtual deberá ser sometida a una terapia psicológica de remediación, orientadas al restablecimiento de su tranquilidad como individuo y persona y para el mejor manejo de este tipo de incidentes.

**Artículo 11 – Para el Actor:** La persona que sea hallada culpable como perpetrador de un acto de Acoso Virtual, deberá de forma accesoria a la pena que le sea impuesta, atender sesiones de atención psicológica, a los fines de tratar sus cuadros o perfiles psicológicos por parte de un especialista. El informe que sea emitido por el psicólogo deberá ser parte del expediente. El sujeto tratado deberá atender las recomendaciones y tratamiento impuesto por el psicólogo. En adición a las terapias la persona que sea hallada culpable como perpetrador de un acto de Acoso Virtual, deberá de cumplir un programa de trabajo social impuesto por el Juez de la causa. Los trabajos sociales contemplados a los efectos de la presente Ley son los siguientes:

1. Cien (100) horas de trabajo comunitario o social, por faltas que no ameriten privación de libertad, pero que sean constitutivos de Acoso Virtual.
2. Doscientas (200) horas de trabajo en el centro de privación de libertad para aquellos casos que el Acoso Virtual contempla una privativa de libertad.

## **Capítulo II**

### **Sanciones**

**Artículo 12. - Entes sancionadores:** La imposición de las sanciones derivadas del incumplimiento de la presente ley será asignada a los tribunales de la Republica que instruyan y conozcan de las causas y dicten sentencia definitiva a tales fines.

**Artículo 13 - Monto de las sanciones:** Sin perjuicio de las responsabilidades penales, las responsabilidades administrativas y civiles que correspondan a todo usuario sujeto que sea impuesto de responsabilidad por acto de Acoso Virtual generarán multas que oscilan entre Trescientas Unidades Tributarias (300 U.T.) y Quinientas Unidades Tributarias (500 U.T.). Las sanciones serán impuestas de forma concurrente a los responsables en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias o atenuantes existentes.

Parágrafo Primero: El Reglamento de la presente Ley determinará las condiciones y procedimientos para la aplicación de las sanciones aquí previstas, las que deberán graduarse con relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando en todo momento el debido proceso.

**Artículo 14 - Sujetos Susceptibles de Sanción:** Serán sujetos de las sanciones contempladas en la presente Ley y de forma conexas las contempladas en la Ley de Delitos Informáticos, todos los directores y accionistas de entes y empresas públicas, los gerentes de informática o tecnología de la información y personal encargado de administrar los sistemas que compongan una Plataforma Tecnológica Gubernamental, si se demuestra que desde aquellas fue generado el hecho o la comisión del acto constitutivo de Acoso Virtual.

**Artículo 15 - Sanción por Reincidencia:** La falta de cumplimiento del tratamiento impuesto por el psicólogo o del trabajo social en el caso que no ameriten privación de libertad, dará lugar a la declaratoria de reincidencia y de la aplicación de una pena de tres (3) meses de arresto con medida sustitutiva de presentación a los fines de dar cumplimiento al tratamiento y trabajo social inicialmente impuesto. La reincidencia generará prisión de seis (6) meses. La falta de cumplimiento del tratamiento impuesto por el psicólogo o del trabajo social en el caso que ameriten privación de libertad, dará lugar al aumento de la pena en un tercio. La reincidencia generará prisión de un (1) año.

## **Título III**

### **Capítulo I**

#### **Disposiciones Transitorias**

**Artículo 16 – Vigencia:** La presente ley entrará en vigor a partir de su fecha de publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Artículo 17 – Reglamento:** El Ministerio Público y la Defensoría del Pueblo de forma conjunta, dictará el Reglamento que desarrolla la presente ley, dentro de los noventa (90) días siguientes a la fecha de publicación del presente cuerpo normativo en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Artículo 18 - Adecuación de Órganos de Control:** El Ministerio Público adecuará su organización de direcciones y su infraestructura tecnológica a los fines de

garantizar el cumplimiento de los principios contenidos en la presente ley y con el propósito de garantizar el cumplimiento de su actividad supervisora, rectora, contralora y ejecutora de los principios y garantías amparados por la presente ley. Dicha adecuación no debe exceder de un plazo de noventa (90) días siguientes a la fecha de publicación del presente cuerpo normativo en la Gaceta Oficial de la República Bolivariana de Venezuela.