Requisitos mínimos para la Ley de Protección de Datos Personales de Ecuador

Este documento presenta un conjunto de reflexiones desarrolladas por la Asociación para el Progreso de las Comunicaciones (APC)[1], Derechos Digitales[2] y Access Now,[3] como organizaciones especializadas en el ámbito de los derechos humanos, en el entorno digital orientadas a alimentar el debate en torno a la normativa de protección de datos personales en Ecuador. Se centran en los mínimos necesarios que, con base en nuestra experiencia, debe comprender dicho proyecto con el objeto de satisfacer estándares adecuados de protección alineados con el respeto de los derechos humanos consagrados en la Constitución y en tratados internacionales ratificados por el Ecuador.

Cabe recordar a este respecto, que en su última visita a Ecuador en el año 2018, el Relator Especial de la Organización de Naciones Unidas para la libertad de expresión, señaló que la Ley de Protección de Datos que se promulgue debe ser coherente con las normas internacionales, haciendo efectivas las garantías del artículo 66 numeral 19 de la Constitución, para el ejercicio de los derechos a la privacidad y la libertad de opinión y expresión.[4]

La demanda por una legislación integral y moderna de protección de datos personales se relaciona, además, con la necesidad de promover la confianza y la certeza jurídica en el uso de datos como base de la economía y la innovación en la sociedad de la información. Asimismo, se requiere como garantía para la autodeterminación de las personas, lo que contribuye a fortalecer y consolidar la democracia y los regímenes basados en el reconocimiento de los derechos humanos.

Es innegable el impacto que ha tenido la entrada en vigor en 2018 del Reglamento General de Protección de Datos (RGPD) en la actualización de las legislaciones de protección de datos en todo el mundo, en la región y, por ende, sobre Ecuador. El RGPD sienta condiciones para

1 https://www.apc.org/
2 https://www.derechosdigitales.org/
3 https://www.accessnow.org/
4 Observaciones Preliminares del Relator Especial de la ONU sobre libertad de expresión después de su visita en Ecuador (5 – 11 de octubre 2018). Disponible en: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=23713&LangID=S

quienes, en un entorno globalizado con crecientes flujos transfronterizos de datos, quieran dinamizar su economía a través del intercambio de bienes y servicios con las garantías adecuadas para la protección de los datos personales de su ciudadanía.

La referencia al RGDP es importante en este contexto porque en el año 2016 se suscribió el Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea (UE), con el objetivo de buscar mejores condiciones para el intercambio de bienes y servicios entre los países miembros de la UE y el Estado ecuatoriano. Ese acuerdo, demanda a Ecuador un nivel adecuado de protección del flujo transfronterizo de datos personales y la existencia de un ente especializado en la protección de datos personales.

En el proceso de elaboración de esta normativa es menester comprender la transversalidad del objeto regulado por la ley de protección de datos personales. Este derecho es transversal y garantiza el libre ejercicio de otros derechos como el de autodeterminación informativa, privacidad, libertad de expresión, participación ciudadana, entre otros. Su objetivo será el establecer reglas para el desarrollo de actividades que involucren la recolección y procesamiento de datos. Así como también, prevenir injerencias arbitrarias en el normal desenvolvimiento de la vida de los ciudadanos, a diferencia de otras regulaciones que buscan de forma reactiva brindar mecanismos de reparación frente a vulneraciones, como sucede con el ya existente habeas data.

A continuación, nos referimos a los aspectos que consideramos indispensables para una ley integral de protección de datos personales, que sentimos requieren de un oportuno énfasis y reforzamiento en la discusión legislativa, luego de examinar el contenido tanto del Proyecto de Ley Orgánica de la Protección de Datos Personales, presentado por el Presidente de la República Lenin Moreno (en adelante, Proyecto número de trámite 379637), como el Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y la Privacidad sobre los Datos Personale, presentado por la Asambleísta Gabriela Rivadeneira (en adelante, Proyecto número de trámite 254848), ambos presentados a la Asamblea Nacional y radicados para su examen en esta Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral.

En efecto, hemos identificado una serie de materias en que teniendo en consideración el texto de las propuestas presentadas creemos conviene hacer una revisión de las mismas a la luz de los mejores estándares desarrollados en la materia a nivel internacional para contar con disposiciones claras que resguarden forma efectiva los derechos de los ciudadanos ecuatorianos.

1. Cuestiones generales

La relación de las personas con sus datos es de titularidad, nunca de propiedad. Ello porque los datos personales son informaciones que se refieren a la persona, sus características, hábitos y relaciones, que se vinculan directamente con la dignidad de ésta, y cuyo control permite a su titular ejercer otros derechos y libertades fundamentales. Es por eso que a nivel internacional se ha entendido que respecto de los datos personales puede haber regímenes de consentimiento o autorización legal de utilización, pero ellos mantienen siempre vinculación con

su titular para habilitarle el ejercicio de sus derechos respecto a éstos, aún de cara a las entidades públicas o privadas que realizan su tratamiento.

La exposición de motivos y el texto de la Ley que se debata y apruebe debe considerar la interconexión entre la protección de datos personales, el acceso a la información y la libertad de expresión. Al mismo tiempo debe tener como eje central el derecho a la autodeterminación informativa de las personas en el contexto de la sociedad de la información y protegerla en forma independiente del derecho a la intimidad.

Por vía ejemplar, el artículo 1 del proyecto número de trámite 254848 establece que el objetivo de la legislación es proteger y garantizar el derecho a la intimidad y privacidad de las personas en el tratamiento de sus datos personales. Si bien la protección de los datos personales muchas veces se encuentra estrechamente vinculada a estos derechos, también corresponde a un derecho fundamental autónomo. En consecuencia, existen casos en los cuales puede existir una vulneración al derecho fundamental a la autodeterminación informativa, pero no a la intimidad de los individuos; por ejemplo, cuando se tratan datos de carácter público utilizados para un fin distinto para el cual fueron recolectados. En consecuencia, sugerimos que el objeto de protección de la ley, se refiera explícitamente al derecho a la autodeterminación informativa, para así evitar limitar su ámbito de aplicación exclusivamente a aquellos casos en que se afecta la intimidad de los individuos.

Por otra parte, de cara a la armonización con el ejercicio de la libertad de expresión y el acceso a la información pública, no consideramos conveniente que la ley incorpore una regulación específica del llamado «derecho al olvido» el cual habilita la remoción de contenido en línea. Desde las organizaciones de sociedad civil, consideramos riesgoso que dentro del régimen de protección de datos personales se contemple la posibilidad de solicitar exclusión de resultados en motores de búsqueda bajo consideraciones de protección a la privacidad o a la reputación. La información que resulte relevante para el interés público nunca debe ser des-indexada o excluida del listado de resultados de búsqueda por cuanto en el Sistema Interamericano de protección de los derechos humanos regido por la Convención Americana de derechos humanos la censura previa se encuentra prohibida, y se ha establecido que el ejercicio abusivo de la libertad de expresión corresponde sea sujeto a mecanismos de responsabilidad ulterior, en los cuales, mediante la intervención judicial, pueda realizarse un balance de los derechos implicados.

La Corte Interamericana de Derechos Humanos ha provisto directrices para la compatibilización de estos derechos en los casos en los cuales ellos pueden entrar en conflicto, indicando los requisitos para determinar cuándo es legítima una restricción del derecho a la privacidad en pos de la libertad de expresión y acceso a la información, señalando al efecto que: “[…] las restricciones que se impongan deben ser necesarias en una sociedad democrática, lo que depende de que estén orientadas a satisfacer un interés público imperativo. Entre varias opciones para alcanzar ese objetivo, debe escogerse aquélla que restrinja en menor escala el derecho protegido. Es decir, la restricción debe ser proporcional al interés que la justifica y debe ser conducente para alcanzar el logro de ese legítimo objetivo, interfiriendo en la menor

medida posible en el efectivo ejercicio del derecho"[5]. En este sentido, resulta legítimo restringir la privacidad, en la medida en que se pruebe que existe un interés público en que la ciudadanía conozca una determinada información, y que haya proporcionalidad entre la relevancia de divulgar los antecedentes y el nivel de afectación a la intimidad.

Cualquier limitación previa al ejercicio de la libertad de expresión se sujeta a un test tripartito: (i) la restricción debe encontrarse establecida en una ley en sentido formal y material, (ii) ser necesaria e idónea para alcanzar un objetivo legítimo, y (iii) y debe ser aplicada en forma proporcional para lograr la menor afectación posible del derecho. Las limitaciones a la libertad de expresión deben además ser ordenadas por un juez o autoridad jurisdiccional competente, independiente e imparcial con todas las garantías del debido proceso. Los Estados deben garantizar el pleno ejercicio de la libertad de expresión tanto fuera como en línea, incluyendo su dimensión individual y social[6].

Por las misma razones, tampoco resulta recomendable que en el marco de la legislación de protección de datos se incluyan normas referidas a la difamación o a la protección del honor, así como tampoco normas que limiten el acceso a información pública o a información sobre el desempeño de funcionarios públicos, puesto que colide con la rendición de cuentas y el derecho de los ciudadanos al acceso a información transparente sobre la gestión pública.

2. Definiciones

La normativa debe incluir definiciones claras respecto a lo que constituye un dato personal y un dato sensible y establecer niveles de protección acorde. Los datos sensibles deben estar definidos de manera no taxativa y mencionar los datos genéticos y biométricos, diagnósticos de salud mental o física, historial sobre sexualidad o vida sexual, historial sobre delitos civiles o penales, afiliación política, afiliación religiosa, como cualquier otro dato que pueda implicar una discriminación arbitraria. El tratamiento de datos sensibles sólo puede autorizarse si los usuarios expresan libremente su consentimiento explícito e informado o si la ley lo autoriza explícitamente en forma proporcional y necesaria a la finalidad legítima perseguida. En ambos casos se deben establecer resguardos respecto de quién tiene acceso, quién puede utilizar esta información y con qué finalidad. Los ciudadanos deben mantener el derecho a rehusarse a que se almacenen sus datos personales sensibles.

3. Categorías especiales de datos

Los datos relativos a niños, niñas y adolescentes corresponden a categorías de datos especialmente protegidos. Por lo mismo, su tratamiento debe estar condicionado al cumplimiento de requisitos restrictivos y que tengan como objetivo la protección de esta categoría de titulares. En este sentido, no corresponde que los datos de niñas, niños y adolescentes puedan ser tratados libremente ni aún por tratarse de datos de naturaleza pública.

5 Corte IDH. Caso Claude Reyes y otros vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párr. 91.
6 Corte IDH. Caso Ricardo Canese vs Paraguay. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 31 agosto 2004, Serie C No. 111, párr. 96.

La normativa debe incluir explícitamente medidas especiales para la protección de los datos de tráfico de las comunicaciones o metadatos y de los datos personales registrados a partir de actividades de internet de los usuarios, debido a que esta información revela rasgos personales particularmente sensibles. Los metadatos contenidos en las comunicaciones telefónicas, en el correo electrónico, en las fotografías digitales o en los registros de acceso a redes sociales permiten identificar a la persona, localizarla geográficamente y revelar las características de los dispositivos que usa, lo que la hace más vulnerable a la vigilancia por parte del Estado o de otros privados. La Ley de Protección de Datos Personales debe incluir disposiciones para regular la captura, almacenamiento y tratamiento de datos que obtienen los dispositivos inteligentes, así como la obligación de proporcionar información clara a los usuarios para que tomen decisiones sobre el uso de estos aparatos.

4. Ámbito de aplicación de la ley

Resulta conveniente dotar a la ley de aplicación extraterritorial de forma que garantice la protección de los datos personales de los ciudadanos ecuatorianos en todo momento aún cuando ellos sean procesados fuera de su territorio. Ello implica garantizar que los usuarios sean respetados sin importar dónde están ubicadas las entidades que utilizan los datos de las personas.

Estas medidas jurisdiccionales pueden evitar una espiral descendente en términos de protección, por la cual ciertas industrias decidirían reubicar sus compañías fuera de un país para evitar la aplicación de medidas que protejan al usuario. Si bien existen múltiples dificultades para su implementación, sería positiva incorporar la extraterritorialidad, por ejemplo, cuando la entidad se encuentre en un territorio jurisdiccional distinto, pero recolecte, procese o trate datos personales de ciudadanos ecuatorianos. Los legisladores deben indicar claramente en qué casos la ley aplicaría fuera de sus fronteras, a qué actores específicamente, qué mecanismos de aplicación de la ley estarían vigentes, y brindar a los usuarios, las compañías, y las autoridades claras vías de reparación.

5. Principios que rigen el tratamiento de datos personales

A continuación listamos algunos de los principios vinculantes de común inclusión a nivel internacional que permite orientar el régimen de protección de datos personales:

a. Legalidad: la información debe ser procesada en una base jurídica clara, con un propósito claro, y de una manera justa y transparente.
b. Limitación de la finalidad: el propósito de la recolección y procesamiento debe ser específico, explícito, y de duración limitada.
c. Minimización de dato: los datos personales recopilados y utilizados deben limitarse a ser suficientes, pertinentes y no excesivos en relación con un propósito específico y definido.
d. Exactitud y calidad: los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados. Los usuarios deben tener el derecho a eliminar, rectificar, y corregir su información personal.
e. Conservación limitada: los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.

f. Seguridad de los datos: los datos personales deben ser procesados de manera que se garantice una seguridad de vanguardia para los datos, junto con la protección contra tratamiento no autorizado o ilegítimo y contra la pérdida accidental, destrucción o daños de los datos, utilizando medidas técnicas y organizacionales pertinentes.
g. Confidencialidad: el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.
h. Transparencia e información: las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.
i. Responsabilidad: quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.

6. Derechos de los titulares de datos personales

La normativa debe incluir una lista de derechos vinculantes de los titulares de los datos para garantizar que tengan control sobre su información personal:

a. Derecho a acceso, para obtener la información de los servicios y compañías con respecto a la posible recopilación y procesamiento de datos personales que los conciernan.
b. Derecho de rectificación de información errónea que le concierne.
c. Derecho de cancelación para solicitar la eliminación de todos los datos identificables vinculados a su persona al momento en que dejan de usar un servicio o aplicación.
d. Derecho de oposición para rehusarse al procesamiento de información personal identificable.
e. Derecho a información clara y entendible por parte de las entidades que procesan sus datos personales.
f. Derecho a obtener información sobre la lógica que subyace en el tratamiento de datos personales automatizados y sus efectos en toma de decisiones.
g. Derecho a la portabilidad que permite que los usuarios movilicen ciertos datos personales que han compartido de una plataforma a otra que ofrezca servicios similares.

El ejercicio de estos derechos debe posibilitarse en forma gratuita, de modo que no se generen desincentivos a su ejercicio.

El derecho de cancelación y de oposición no pueden ser restringidos a hipótesis en que el tratamiento no haya respetado los principios, derechos o garantías constitucionales o legales, sino que deben encontrarse siempre disponibles. Esto porque al tratarse de un ejercicio de autodeterminación informativa, la posibilidad de que los titulares revoquen su consentimiento

existir siempre sin la necesidad de invocar un fundamento, es decir, debe quedar entregada a su mera voluntad.

Por otra parte, el derecho a portabilidad es un sello de las legisladoras más a la vanguardia en materia de protección de datos personales que permite a los titulares exigir la entrega de sus datos personales en un formato estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos. De esta forma, el titular puede decidir cambiar de proveedor de servicio de forma más rápida y expedida, aumentando los niveles de competitividad de los sectores económicos basados en el tratamiento de datos personales y generando mejores condiciones de protección y decisión para los consumidores.

7. Obligaciones de los responsables de bases de datos

La ley de protección de datos personales debe establecer con precisión que quienes están encargados del tratamiento de nuestros datos son legalmente responsables por el tratamiento de los mismos y por asegurar que su recolección, procesamiento y uso no ocurra en detrimento de la realización de los derechos de las personas. Esto implica que la ley debe establecer explícitamente obligaciones de notificación de filtración, daño y fuga de datos personales.

También implica establecer mecanismos obligatorios de protección de la seguridad de los datos, incluyendo medidas de solución y reparación en caso de que ocurran filtraciones o algún otro tipo de falla de seguridad. También requiere exigir que la privacidad y la protección de datos sean tomadas en cuenta por los ingenieros en la fase de diseño de productos y servicios, y que estén configurados en el nivel de protección más alto por defecto: este es el concepto de protección de datos por diseño y por defecto. Estas nociones deben estar detalladas en la ley para solicitar que las entidades las adopten, teniendo en consideración el estado de la técnica, los costos de implementación, la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos asociados al tratamiento.

8. Autoridad de Control

Se debe crear o dotar a una institución existente de independencia que tenga mecanismos robustos para garantizar la aplicación de la ley a todo ente público o privado que recolecte y procese datos personales. Esto implica garantizar que la autoridad encargada de la aplicación de la ley se encuentre libre de cualquier injerencia, sea autónoma, con presupuesto propio y especializada, es decir, con personal técnico con conocimientos en la materia.

Si bien puede considerarse un diseño institucional válido alojar la autoridad de control dentro de organismos previamente existentes con dependencia en algún Ministerio, debe tenerse en consideración que tal modelo no permitiría a Ecuador optar a ser considerado por la Unión Europea como un país adecuado para la transferencia transfronteriza de datos personales, lo que puede repercutir negativamente en la competitividad de sectores económicos relacionados con modelos de negocio basados en la tecnología y el procesamiento de datos.

Para alcanzar este estatus, sería recomendable que la Autoridad Nacional de Protección de

Datos Personales sea un organismo autónomo, de carácter técnico especializado y con patrimonio propio. Este diseño institucional entrega mayores garantías que las decisiones respondan a criterios técnicos, con independencia del gobierno de turno.

Resultaría relevante que se asegure que la Autoridad de control cuente con facultades para dictar normativa de carácter sectorial, en la forma de resoluciones administrativas, de forma tal que esta pueda dar a conocer a la industria sus interpretaciones de ciertas disposiciones específicas o su aplicación a casos particulares, otorgando mayor certeza jurídica a los actores del mercado. Por otro lado, sería positivo que la Autoridad estuviese a cargo de coordinar la cooperación internacional en materia de protección de datos personales con otros países y organismos internacionales. Por último, corresponde que sea la Autoridad la institucionalidad encargada de resolver las contiendas entre titulares y responsables de bases de datos, en aquellos casos en que el responsable no ha respondido a la solicitud del titular en el plazo establecido o lo ha hecho de forma incompleta.

La Autoridad de Protección de Datos Personales debe recibir el mandato para llevar a cabo investigaciones y accionar ante reclamaciones, emitiendo pedidos vinculantes e imposición de sanciones cuando toma conocimiento de que una compañía, institución o algún otro organismo ha quebrantado la ley. Este mandato incluye ser capaz de: exigir información al responsable o el encargado del tratamiento, realizar auditorías, obtener acceso a toda la información que se requiera para la finalidad de la investigación, incluido el acceso físico a las instalaciones.

Tanto los ciudadanos individuales como las organizaciones de la sociedad civil deben tener garantizado el derecho a solicitar a la Autoridad de Protección de Datos Personales que realicen investigaciones y/o apliquen sanciones frente a evidencias de vulneración de la ley.

La Ley debe prever que la Autoridad de Protección de Datos Personales tendrá obligaciones de transparencia con respecto a la información global sobre el número de solicitudes de datos hechas por entes del Estado tanto a agentes privados como públicos, aprobadas y rechazadas, con especificación de sus propósitos.

9. Excepciones a la aplicación de ley limitadas

La legislación que se establezca debe definir los requisitos para el tratamiento legítimo de datos personales, y cualquier excepción que se establezca debe ser descrita de forma precisa y acotada, operando de manera excepcional y no en forma genérica para una categoría completa de datos o de agentes involucrados en su tratamiento.

Debe restringirse las excepciones a la aplicación de la ley que permitan al Estado la recopilación y procesamiento de excesiva información sobre los ciudadanos bajo el alegato de razones de “seguridad nacional”. La ley debe garantizar que el Estado sólo requiera los datos estrictamente necesarios, por el tiempo necesario, para suministrar servicios que requieren los ciudadanos. Asimismo, debe haber garantías de que esos datos sean almacenados de manera segura y sólo sean compartidos con otras instituciones públicas por razones legítimas, en los casos establecidos por la ley, previa autorización de una autoridad judicial competente o

consulta vinculante con la autoridad de protección de datos.

Respecto de esta cuestión, resulta problemático que el artículo 2 inciso segundo del proyecto número de trámite 254848 opte por no hacer aplicable las disposiciones de la ley a cierto tratamiento de datos: seguridad nacional, orden y seguridad, salud pública y derechos de terceros. Por su parte el proyecto número de trámite 379637 en su artículo 37 consagra la posibilidad de exceptuar de aplicación de la normativa a solicitudes administrativas en forma amplia, con lo cual se vacía la obligatoriedad de cumplimiento de la normativa por organismos públicos.

10. Excepciones al consentimiento limitadas

De igual forma la ley debe incluir limitación del uso de "interés legítimo" para el tratamiento de datos por parte de empresas privadas sin autorización explícita de las personas. Debe incluirse la obligatoriedad de obtener consentimiento explícito si se desea utilizar los datos de un usuario para la elaboración de perfiles, así sea con fines de mejoramiento del servicio, atención al cliente o mercadeo. Asimismo, debe incluirse la obligatoriedad de obtener consentimiento explícito si se van a ceder bases de datos a terceros para cualquier finalidad.

En este sentido, resulta deficiente lo establecido en el artículo 3.4 del proyecto número de trámite 254848, que establece que el consentimiento no será requerido cuando los datos provengan de fuentes públicas de información o se recaben para funciones propias de las instituciones del Estado. Estas excepciones resultan excesivamente amplias y se basan en conceptos que no están debidamente definidos en la ley. Se recomienda definir qué se entenderá por “fuentes públicas de información”, estableciendo una lista taxativa de categorías de bases de datos que cumplen dicha condición. Asimismo, se recomienda acotar el concepto de “funciones propias de instituciones del Estado”, limitándolas a aquellas atribuciones establecidas explícitamente por las leyes que regulan los distintos organismos públicos.

11. Flujo transfronterizo de datos

La Ley de Protección de Datos Personales debe considerar las posibles salvaguardas para extender la protección a los flujos transfronterizos de los datos de los ciudadanos ecuatorianos. Estos mecanismos deben estar sometidos a una supervisión estricta y transparente, e incluir medidas de reparación para garantizar que los derechos de los usuarios viajen junto con los datos.

Por ejemplo, el artículo 20 del del proyecto número de trámite 254848 establece que la transferencia internacional de datos personales sólo será permitida cuando el país receptor proporcione cierto nivel de protección de datos. Sin embargo, no establece un criterio objetivo para realizar dicha ponderación, como si lo hace el artículo 65 del proyecto número de trámite 379637. Por otro lado, se recomienda que la Autoridad Nacional de Protección de Datos sea la encargada de generar y actualizar un listado de países que cuentan con un nivel adecuado de protección.

12. Régimen Sancionatorio

El principal objetivo de establecer un régimen de multas para el incumplimiento de disposiciones legales es que estas sean disuasivas, de forma tal que los participantes del mercado no las puedan incorporar como costos en su modelo de negocio. El establecimiento de un régimen sancionatorio a las faltas contra la Ley de Protección de Datos Personales además debe ser conmensurado con la magnitud de la falta y las características del infractor (público o privado).

En este sentido, una multa máxima de diez salarios básicos unificados como la que establece el proyecto número de trámite 254848 no parece ser un monto de una cuantía suficiente para resultar realmente disuasivo. Se recomienda que el régimen sancionatorio se base en tramos de distinta cuantía para las sanciones leves y graves. Del mismo modo, sería positivo crear la categoría de infracción gravísima, reservada para aquellas conductas realizadas de mala fe o de carácter reincidente. Respecto de las infracciones graves y gravísimas, el monto de la multa debería estar calculado en base a un porcentaje del volumen de negocio de la entidad infractora, correspondiente al ejercicio anual anterior. En subsidio, la multa para las infracciones graves y gravísimas puede calcularse en base a un porcentaje de las utilidades de la entidad obtenidas en el ejercicio anual anterior.

Todo ello porque las sanciones deben tener entidad suficiente para generar un efecto disuasivo que garantice el efectivo cumplimiento de la norma. Asimismo, deben establecerse con claridad los mecanismos de reclamo accesibles y de bajo costo a los que puede apelar el ciudadano cuando sea ha producido una infracción de sus derechos.

Petitorio

Requerimos tengan en consideración estos aporte al momento de debatir las disposiciones propuestas por el proyecto número de trámite 254848 y el proyecto número de trámite 379637, con la finalidad de que la normativa de protección de datos que se apruebe en definitiva refleje los elementos esenciales para asegurar a los titulares control sobre sus datos y garantizar el ejercicio de los derechos de todas y todos los ecuatorianos.