



"Por una Ley Protección de Datos centrada en los derechos del ciudadano".

Notas para la discusión del Anteproyecto de Ley de Protección de Datos Personales de Ecuador

La Asociación para el Progreso de las Comunicaciones (APC), Access Now, Derechos Digitales y el ObserLatInf proponen los siguientes puntos para orientar el debate entre las múltiples partes interesadas sobre **el Anteproyecto de Ley de Protección de Datos Personales de Ecuador**.

Antecedentes

Desde 1988, el Comité de Derechos Humanos de las Naciones Unidas reconoció la necesidad de una legislación sobre protección de datos en concordancia con el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos que dice:

La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por autoridades públicas como por particulares o entidades privadas, deben estar reglamentados por la ley... Toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos... se han compilado o tratado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.

En Ecuador, la protección de datos es un derecho fundamental. La Constitución de Ecuador en su Art. 66, numeral 19, establece que se reconoce y garantizará a las personas "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización

"Por una Ley Protección de Datos centrada en los derechos del ciudadano"

#ProtecciónDatosEC [HTTP://OBSERLATINF.ORG/PROTECCION-DE-DATOS](http://OBSERLATINF.ORG/PROTECCION-DE-DATOS)

el titular y el mandato de la ley". Paradójicamente, la estructura legal del país es absolutamente deficiente para garantizar dicha protección.

En ese sentido, las Observaciones Preliminares del Relator Especial de la ONU sobre libertad de expresión después de su visita en Ecuador (5 – 11 de octubre 2018) destacan que la Ley de Protección de Datos 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.

La protección de datos personales es uno de los 6 ejes fundamentales del Plan de la Sociedad de la Información y del Conocimiento de Ecuador. En ese documento de política pública se establece la necesidad de contar con un marco integral, que impulse a la sociedad ecuatoriana hacia una cultura de protección de datos personales y el uso adecuado de las tecnologías de la comunicación e información, garantizando un ambiente que permita el desarrollo integral y proteja la dignidad de todos sus ciudadanos dentro del libre flujo de información que fomente la reactivación económica, promueva procesos de innovación y mejore la calidad de los servicios.

Internacionalmente, la protección de datos personales que hacen identificables a los individuos implica establecer reglas que deben cumplir todas las entidades públicas y privadas que capturen, almacenen o procesen datos de los ciudadanos. La demanda de legislación de protección de datos personales se relaciona con la necesidad de desarrollar confianza en el uso de datos como base de la economía y la innovación en la sociedad de la información, así como también desarrollar confianza para la acción ciudadana en la esfera pública y para la participación en los asuntos públicos. Asimismo, se requiere como garantía para la autodeterminación de las personas, los que contribuye a fortalecer y consolidar la democracia y los regímenes basados en el reconocimiento de los derechos humanos.

Es importante determinar la manera en la que la ley de protección de datos personales en el Ecuador responderá a esos imperativos de la globalización. Ecuador es uno de los países de América Latina que no cuenta con una Ley de Protección de Datos Personales, situación que también ocurre en los casos de Venezuela y Bolivia.

Las autoridades ecuatorianas reconocen el impacto de 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 y por ende su efecto sobre Ecuador. El RGPD sienta condiciones para 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. Ya en la actualidad, empresas ecuatorianas que tratan con datos de ciudadanos europeos están obligados a cumplir con el RGPD. La referencia al RGPD es aún más importante estratégicamente porque en el año 2016 se suscribió el *Protocolo de Adhesión de Ecuador al*

"Por una Ley Protección de Datos centrada en los derechos del ciudadano"

#ProtecciónDatosEC [HTTP://OBSERLATINF.ORG/PROTECCION-DE-DATOS](http://OBSERLATINF.ORG/PROTECCION-DE-DATOS)

Acuerdo Comercial Multipartes con la Unión Europea, 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.

Consideramos que la apertura de los decisores de política pública para recoger los planteamientos de la sociedad civil, así como de las demás partes interesadas, es crucial para desarrollar una legislación orientada por la protección de derechos. La Dirección Nacional de Registro de Datos Públicos (DINARDAP) inició en abril de 2018 un proceso de desarrollo de un anteproyecto de ley en la materia de Protección de Datos, en el cual ha habido espacios para la participación de la sociedad civil. No obstante, observamos la limitación de que no ha habido una difusión pública más amplia de la importancia de esta legislación, que incide sobre prácticamente toda la economía de comercios y servicios, así como sobre todas las instancias en las cuales los ciudadanos tienen relación con el Estado. Igualmente, ha sido una limitación para la participación sustantiva el que no se haya contado hasta el momento con un borrador del articulado. Sostenemos que en los procesos de desarrollo de legislación, se puede estar de acuerdo a nivel de los principios y los conceptos, sin embargo es en el lenguaje y redacción del articulado en el que se juega el sentido de la ley.

Objetivos

Desde las organizaciones de la sociedad civil que trabajan en la promoción y defensa de derechos digitales, que suscriben este documento, nos proponemos:

- *Promover una legislación de protección de datos con enfoque de derechos y centrada en los ciudadanos, que contribuya al ejercicio de derechos fundamentales, tales como los derechos a la libertad de expresión, la participación, la libre asociación y el acceso a la información pública.*
- *Promover un proceso de elaboración de la Ley de Protección de Datos Personales que sea participativo, inclusivo y transparente, con amplias consultas a las múltiples partes interesadas.*
- *Facilitar la participación significativa de los grupos de la sociedad civil en consultas públicas del proyecto de ley y mesas redondas de expertos en protección de datos, a fin de que se le dé máxima consideración en la elaboración de anteproyecto a las propuestas de organizaciones de la sociedad civil y a la consideración de las observaciones de expertos internacionales en la formulación de políticas públicas para la protección de datos.*

"Por una Ley Protección de Datos centrada en los derechos del ciudadano"

#ProtecciónDatosEC [HTTP://OBSERLATINF.ORG/PROTECCION-DE-DATOS](http://OBSERLATINF.ORG/PROTECCION-DE-DATOS)

- *Promover la aplicación efectiva de la ley con la creación de una autoridad de protección de datos personales bajo criterios de independencia, autonomía y especialización técnica en el marco establecido por la Constitución de Ecuador, en consideración de lo cual optamos por apoyar la creación de una autoridad que deberá contar con los recursos y poderes para desarrollar sus actividades.*

Aspectos prioritarios para el texto del proyecto de Ley

Las organizaciones de la sociedad civil que suscriben el documento proponemos establecer como prioridades para un proyecto de ley orientado a la garantía de derechos las siguientes:

1. Desarrollo de una Ley de Protección de Datos Personales que se fundamente en un enfoque de derechos humanos teniendo como eje central a las personas y sus derechos. La exposición de motivos y el texto de la Ley deben considerar la interconexión entre la protección de datos personales, el acceso a la información y la libertad de expresión. Asimismo, debe armonizarse con otros derechos individuales relacionados reconocidos en la Constitución de Ecuador, como son: el derecho a la integridad personal; el derecho a guardar reserva sobre las convicciones individuales; el derecho a asociarse, reunirse y manifestarse en forma libre; y, el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual (o digital).
2. Proponemos que en la motivación de la Ley se establezca como eje central el derecho a la autodeterminación informativa de las personas en el contexto de la sociedad de la información. La autodeterminación informativa consiste en un derecho fundamental que garantiza el control de la información personal en registros públicos y privados, no importando el soporte o lugar donde se encuentren o almacenen.
3. Incluir en la legislación claras definiciones de los principios básicos de la protección de datos, entre las cuales debe destacarse:
 - a. limitación de la recopilación y procesamiento de datos para fines específicos y legítimos tanto por agentes públicos como privados, bajo estándares de proporcionalidad que permitan ponderar el fin legítimo perseguido con el grado de afectación de los derechos en juego, como resulta de la jurisprudencia de órganos internacionales de protección de derechos humanos;
 - b. minimización de la recopilación de datos por el sector público y el sector privado a lo requerido para cumplir con propósitos de servicios específicos, procedimientos reglados en la ley y supervisados por la autoridad de control, para compartir tales datos entre servicios.
4. En la Ley de Protección de Datos Personales de Ecuador requerimos normas que garanticen:
 - a. **Transparencia.** Los usuarios deben ser siempre informados en forma previa a que puedan otorgar su consentimiento en la recogida, tratamiento, uso y almacenamiento de sus datos personales.

"Por una Ley Protección de Datos centrada en los derechos del ciudadano"

#ProtecciónDatosEC [HTTP://OBSERLATINF.ORG/PROTECCION-DE-DATOS](http://OBSERLATINF.ORG/PROTECCION-DE-DATOS)

- b. **Finalidad.** Los datos deberán ser recopilados y procesados sólo para fines específicos, explícitos y de duración limitada informados al solicitar el consentimiento por su titular. Nuevas finalidades de uso requieren de una nueva autorización por parte del titular de los mismos.
 - c. **Integridad y confidencialidad.** Los sistemas deben garantizar la protección contra tratamiento no autorizado o ilegítimo, tanto por operadores del sistema como por terceros, así como contra la pérdida, destrucción o daños de los datos.
- 5. Establecer explícitamente los derechos de las personas naturales, especialmente los siguientes:
 - a. derecho de acceso que habilite a los usuarios a obtener información con respecto a la recopilación y procesamiento de datos personales que les conciernan simplemente con solicitarlo a las agencias de servicios públicos y compañías privadas;
 - b. derecho a oponerse al procesamiento de datos personales;
 - c. derecho a solicitar la eliminación de todos los datos personales al momento en que dejan de usar un servicio o aplicación;
 - d. derecho de rectificación de datos personales erróneos que le conciernen;
 - e. derecho a información clara y entendible, previa a la recolección, 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 permita a los usuarios movilizar ciertos datos personales que han compartido en una plataforma a otra que ofrezca servicios similares usando formatos que resulten interoperables.
 - h. establecimiento explícito del derecho a eliminar, rectificar y corregir información personal recopilada tanto por agencias del Estado, como agentes privados.
- 6. Crear una autoridad de supervisión independiente que tenga mecanismos robustos para garantizar la aplicación de la ley. La efectividad de un régimen de protección de datos personales depende en gran medida del establecimiento de una autoridad de control con competencias efectivas para supervisar su cumplimiento e independiente en términos políticos, administrativos y económicos respecto al gobierno de turno. Esto implica que la autoridad de protección debe crearse bajo una normativa que garantice su independencia del Estado y del sector privado, así como su autonomía, para lo cual debe contar con un presupuesto propio y personal especializado en la protección de datos personales. Adicionalmente, es necesario dotar a la autoridad de datos personales de la capacidad técnica para supervisar/fiscalizar a actores públicos y privados, y sancionar el cumplimiento de las medidas de seguridad.
- 7. La Autoridad de Protección de Datos Personales debe tener potestad para llevar a cabo investigaciones *de oficio* y accionar ante reclamaciones, emitir pedidos vinculantes e imponer sanciones cuando toma conocimiento de que una empresa, una institución o algún otro organismo ha quebrantado la ley. Este mandato incluye ser capaz de: exigir información al responsable o el encargado del tratamiento, exigir una respuesta de los responsables o encargados 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 y disponer sanciones significativas, según lo amerite, para disuadir el incumplimiento de la ley.

8. Tanto los ciudadanos 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, bajo procedimientos expeditos, simples y que no impliquen costos excesivos.
9. Limitar la inclusión en la Ley de Protección de Datos Personales de excepciones que permitan al Estado la recopilación y procesamiento de datos personales bajo justificaciones de razones de "seguridad nacional o seguridad pública". Se deben establecer garantías para que los entes del Estado sólo puedan requerir los datos estrictamente necesarios para el ejercicio de sus funciones legítimas autorizadas por ley, en la proporción y 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 y conforme al dictamen que autorizó dicho tratamiento, previa consulta vinculante con la autoridad de protección de datos.
10. La Ley de Protección de Datos Personales debe servir de garantía para prevenir el establecimiento de sistemas de vigilancia masiva de las comunicaciones electrónicas de los ciudadanos. Asimismo, debe prevenir el tratamiento inadecuado de datos personales que se encuentren en registros públicos, con fines que excedan la finalidad bajo el cual tales datos fueron originalmente recogidos, y que resulte en infracción de derechos de sus titulares, entre ellos discriminación política.
11. La Ley de Protección de Datos Personales debe considerar limitaciones al "interés legítimo" como base de legalidad para el tratamiento de datos por parte de empresas privadas sin autorización explícita de las personas afectadas. Debe incluirse la obligatoriedad de obtener consentimiento explícito si se desea utilizar los datos de un usuario para elaborar perfiles de estilos de vida, 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.
12. Incluir medidas especiales explícitas para la protección de datos sensibles. Los datos sensibles revelan rasgos que exponen los aspectos más esenciales de la identidad de la persona y que si son manipulados comprometen gravemente su dignidad y capacidad de autodeterminación.

La Ley de Protección de Datos Personales debe definir explícitamente como datos sensibles:

- datos genéticos
- datos biométricos
- diagnósticos de salud mental o física
- historial sobre sexualidad o vida sexual
- historial sobre delitos civiles o penales
- afiliación política

El tratamiento de datos sensibles sólo puede autorizarse para categorías limitadas establecidas previamente en la ley y sólo si los usuarios expresan libremente su consentimiento de forma explícita, incluyendo especificaciones para controlar quién tiene acceso, quién puede utilizar esta información, con qué finalidad y por cuánto tiempo, que queden documentadas por escrito o digitalmente. Los ciudadanos deben mantener el derecho a rehusarse a que se almacenen sus datos personales sensibles y a solicitar la eliminación de los que hayan sido recopilados si deciden retirar su consentimiento con posterioridad.

13. Incluir explícitamente medidas especiales para la protección de los datos de comunicación o metadatos de las comunicaciones, incluyendo aquellos que se generen a partir de actividades de internet de los objetos. Los metadatos contenidos en las comunicaciones telefónicas, en el correo electrónico, en las fotografías digitales o en los registros de acceso a *social media* son datos personales que permiten identificar a la persona, geolocalizarla y revelar las características de los dispositivos que usa, con lo cual posibilita conocer sus comportamientos y redes de relaciones, con ello la persona resulta más vulnerable a la vigilancia por parte del Estado o de agentes extra-estatales. La Ley de Protección de Datos Personales debe incluir disposiciones sobre 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 y de las aplicaciones que realizan recolección de datos.
14. La Ley de Protección de Datos Personales no debe incorporar provisiones del «derecho al olvido» para habilitar la remoción de contenido en-línea, dado que esas provisiones generan violaciones al derecho a la libre expresión y a la libertad de acceso a la información. Desde las organizaciones de sociedad civil, nos oponemos a que se reconozca dentro de la protección de datos personales la posibilidad de solicitar exclusión de resultados en motores de búsqueda bajo el alegato de protección de la privacidad o de la reputación. La información que resulte relevante para el interés público nunca debe ser des-indexada o excluida de listados de resultados de búsqueda.
15. La Ley de Protección de Datos Personales no debe usarse como vehículo para introducir normas referida 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.
16. La Ley de Protección de Datos Personales debe establecer con precisión que quienes están encargados del tratamiento de los datos son legalmente responsables por asegurar que su recolección, procesamiento y uso no ocurra en detrimento de la realización de los derechos de las personas. Deben incluirse medidas de prevención, solución, reparación y notificación al usuario en caso de que ocurran filtraciones o algún otro tipo de falla de seguridad, interna o provocada por terceros.
17. Deben establecerse obligaciones de seguridad que protejan la confidencialidad, integridad y disponibilidad de los datos. Los datos personales deben ser procesados con

técnicas que garanticen la seguridad desde el diseño de las bases de datos y que queden preconfiguradas en las aplicaciones de tratamiento.

18. La Ley de Protección de Datos Personales debe centrarse en los titulares de los derechos y no en el territorio en donde se encuentra la información. En este sentido, debe considerar salvaguardas para extender la protección a los flujos transfronterizos de los datos de los ciudadanos ecuatorianos y de los ciudadanos extranjeros (residentes o no) que reciben servicios de empresas ecuatorianas o del Estado ecuatoriano.
19. La Ley de Protección de Datos Personales debe establecer mecanismos de transparencia y reporte de solicitudes de datos recabados por el Estado para una finalidad específica y que sean requeridos por agentes del Estado previo dictamen de la autoridad judicial competente. La Ley debe prever que la autoridad de protección de datos tendrá competencias para requerir a las distintas agencias públicas la información agregada sobre el número de solicitudes de datos hechas por cada ente del Estado tanto a agentes privados como públicos. La autoridad de protección de datos deberá publicar informes de transparencia sobre las solicitudes que procese y las investigaciones de oficio que realice.
20. La Ley de Protección de Datos Personales debe establecer un régimen sancionatorio administrativo a las faltas contra la Ley de Protección de Datos Personales, que sea conmensurado con la magnitud de la falta y las características del infractor (público o privado). Asimismo, deben establecerse con claridad los mecanismos de reparación a los que puede apelar el ciudadano cuando se ha producido infracción a sus derechos establecidos en esta ley, se vulnera la debida protección a sus datos o se afecta el disfrute de otros derechos por un inadecuado tratamiento de sus datos.

Se adhieren al documento las siguientes organizaciones:

"Por una Ley Protección de Datos centrada en los derechos del ciudadano"

#ProtecciónDatosEC [HTTP://OBSERLATINF.ORG/PROTECCION-DE-DATOS](http://OBSERLATINF.ORG/PROTECCION-DE-DATOS)