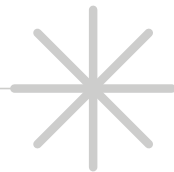


DOCUMENTO DE ANÁLISIS

PRIVACIDAD Y PROTECCIÓN DE DATOS

PROPUESTAS PRE-ELECTORALES 2024-2025

**PROYECTO:
CAMINOS POSIBLES PARA LOS
DERECHOS DIGITALES EN BOLIVIA**



Este documento fue elaborado por el equipo de la Fundación InternetBolivia.org con el apoyo de Asociación Aguayo y el Fondo de Derechos Digitales.

Revisión:

- * Lisette Balbachan
- * Sabrina Lanza
- * Cristian León
- * Lu An Mendez
- * Carolina Perez
- * Nicole Sanchez
- * Cielito Saravia

Diseño:

- * Marcelo Lazarte

Septiembre de 2024

Elaborado por:



Con apoyo de:



Este trabajo se distribuye con licencia Reconocimiento 4.0 Internacional (CC BY 4.0)



Esto significa que usted es libre de:

Compartir - copiar y redistribuir el material en cualquier medio o formato

Adaptar - remezclar, transformar y construir a partir del material para cualquier propósito, incluso comercialmente (La licencianta no puede revocar estas libertades en tanto usted siga los términos de la licencia).

Bajo las condiciones siguientes:

Atribución - Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licencianta o lo recibe por el uso que hace.

No hay restricciones adicionales - No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Acceda a una copia completa de la licencia en:

<https://creativecommons.org/licenses/by/4.0/legalcode.es>

DOCUMENTO DE ANÁLISIS

PRIVACIDAD Y PROTECCIÓN DE DATOS

PROPUESTAS PRE-ELECTORALES
2024-2025

PROYECTO:
CAMINOS POSIBLES PARA LOS
DERECHOS DIGITALES EN BOLIVIA



Índice

1.	INTRODUCCIÓN	2
2.	LA SITUACIÓN DE LA PROTECCIÓN DE DATOS Y PRIVACIDAD EN BOLIVIA	4
3.	LA PROTECCIÓN DE DATOS COMO DERECHO HUMANO	7
	A. LEGISLACIÓN EXISTENTE	8
	B. NECESIDADES Y ARGUMENTOS PARA UNA LEY DE PROTECCIÓN DE DATOS PERSONALES	10
4.	ACCIONES IMPULSADAS PARA LOGRAR LA PROTECCIÓN DE DATOS	11
	A. DESDE SOCIEDAD CIVIL	11
	B. DESDE EL ESTADO	12
5.	HACIA LA CONSTRUCCIÓN DE PROPUESTAS ELECTORALES	14

Introducción

A partir de la pandemia, Bolivia afronta una acelerada transformación digital. Este proceso ha implicado tanto beneficios en relación a las potencialidades que traen las tecnologías, pero también vulneraciones a los derechos humanos debido a la falta de salvaguardas y garantías.

Varias de esas vulneraciones tienen que ver con la afectación directa a la privacidad e intimidad de las personas y/o la exposición de sus datos personales sin su consentimiento. Desde antes de la pandemia, ya existía preocupación con respecto a cómo se estaban recolectando grandes cantidades de datos personales para temas crediticios/ financieros, seguros de diversa índole, marketing y publicidad, entre otros. El mismo hecho de la gran cantidad de fotocopias de CI para diversidad de trámites con entidades públicas y privadas, genera desconcierto por la exposición a terceros de datos como direcciones, números de CI, firmas e incluso huellas digitales. Se sabía que, debido a la falta de adecuados controles y medidas de seguridad, era incluso posible comercializar bases de datos que incluían información sensible de miles de bolivianos/as en espacios tan inusitados como Facebook marketplace o en otros de comercio electrónico.

Por otro lado, desde 2018, con la Ley 1057, que establece el intercambio de datos (interoperabilidad) entre el Servicio de Registro Cívico (SERECI) y el Servicio General de Identificación Personal (SEGIP), y la implementación de la Ciudadanía digital, se aceleró el proceso de digitalización del Estado, requiriendo medidas de protección y mecanismos de transparencia con respecto al manejo de datos que brinden total seguridad a la ciudadanía. Por la anterior razón, desde ese año, se inició una campaña desde sociedad civil¹ para promover la aprobación de una Ley de protección de datos personales. La Agencia de Gobierno Electrónico (AGETIC), ese mismo año y aceptando esta necesidad, por su lado, impulsó un proceso de elaboración de un anteproyecto. Así, en 2019, la Fundación InternetBolivia.org presentó una propuesta de anteproyecto ante la Asamblea Legislativa².

La pandemia intensificó el uso de las tecnologías y con ellas las transacciones de información. Al haber un uso más intensivo de plataformas digitales para la comunicación interpersonal, la educación, el trabajo remoto y el comercio, aumentó proporcionalmente el registro e intercambio de datos personales a través de pasarelas de pago, redes sociales, e incluso vía aplicaciones de mensajería como WhatsApp. Era considerado normal y del día a día, compartir por ejemplo, capturas de los carnets de identidad y otros documentos, información referente a cuentas bancarias, datos de salud, fotografías personales e íntimas, entre otras. Al mismo tiempo, el contexto de pandemia

1 <https://misdatos.internetbolivia.org/linea-de-tiempo/>
<https://www.lostiempos.com/actualidad/pais/20180704/que-son-derechos-digitales-ciudadania-digital>
<https://oxigeno.bo/pol/K3%ADtica/28783>

2 https://misdatos.internetbolivia.org/docs/anteproyecto_ley_de_proteccion_datos_personales_InternetBolivia.pdf

y de crisis política, hizo que el Estado implemente mayores mecanismos de vigilancia y monitoreo de las personas sin medidas de proporcionalidad o legalidad. El gobierno boliviano aumentó sus niveles de seguimiento epidemiológico, las bases de datos, e intentó generar normativa para regular los discursos en redes sociales. Varios años después de la pandemia, esos datos personales siguieron circulando y empezaron a ser compartidos sin ningún tipo de cuidado y con riesgo de ser filtrados hacia terceros.

El intercambio y tratamiento de datos personales aumentó pero no se dieron los mecanismos de regulación, ni las garantías para la personas. La población no puede hacer seguimiento a cómo se usa esa información, oponerse a que sus datos sean recolectados, manejados y hasta comercializados, y ni siquiera pueden demandar que al menos se requiera su consentimiento informado. Si los datos personales se usan para fines lícitos o ilícitos, es algo que escapa a la capacidad de control de la ciudadanía, afectando directamente a sus derechos de privacidad, intimidad, entre otros.

Es así que, en los últimos años, se empezaron a registrar múltiples situaciones de vulneraciones a la privacidad. Se registraron, por ejemplo, usos indebidos de información por parte del Estado, algunas incluso para fines de persecución política, múltiples situaciones de ciberestafas cuya forma de operación es aprovechar información personal, casos de acoso y violencia digital a mujeres y niños, niñas y adolescentes, mala utilización de información por parte de empresas para contactar personas de manera reiterativa y sin consentimiento, entre tantas otras.

El salto hacia los modelos de Inteligencia Artificial y una mayor automatización de procesos informáticos, requieren tecnologías intensivas en datos. Así también el autoaprendizaje mismo que permite incrementar la precisión de sus respuestas y demanda mayor acceso a la información de las personas.

Es necesario que Bolivia pueda contar con una adecuada normativa, a la par de la regulación que ya se ha aprobado en la mayoría de los países del mundo, que resguarde la información privada de las personas, la proteja de las vulneraciones que puedan darse y fortalezca los mecanismos de control, seguridad y transparencia. Tomando en cuenta ello, se busca armar propuestas específicas basadas en evidencia que puedan ser incluidas en los diferentes programas y propuestas de gobiernos en el marco de los procesos electorales en Bolivia 2025-2026.

Esta iniciativa que parte del proyecto “Caminos posibles para los derechos digitales en Bolivia”, es un esfuerzo conjunto de la Fundación InternetBolivia.org apoyada por Asociación Aguayo, Derechos Digitales y el Fondo de Derechos Digitales. Para su elaboración se hizo una revisión exhaustiva de toda la experiencia y conocimientos generados en más de 5 años de trabajo de la Fundación InternetBolivia.org en la campaña “Yo protejo mis datos”. Esta experiencia buscó ser sintetizada y presentada a especialistas y activistas para que pueda ser transformada en ideas específicas como resultado de un breve ejercicio de escenarios prospectivos.

LA SITUACIÓN DE LA PROTECCIÓN DE DATOS Y PRIVACIDAD EN BOLIVIA

Si bien no se cuenta con un registro pormenorizado y sistemático de vulneraciones a los derechos a la privacidad, intimidad y la protección de datos, se han observado en los últimos años varios casos de relevancia. Algunos de estos fueron reportados por los medios de comunicación, y fueron registrados en el portal: <https://misdatos.internetbolivia.org/>.

Desde la década de 2010, en plena emergencia de las plataformas de redes sociales, se han observado diferentes incidentes que dan cuenta de la necesidad de reforzar mecanismos de protección de información. En Bolivia, fueron mediáticos los casos de divulgación de información sensible referente al estado de salud de una ex autoridad de un miembro del Tribunal Constitucional³, y la exposición de material íntimo de una periodista y presentadora de televisión. Ambos hechos flagrantes con respecto a abusos a la intimidad. En 2016, tuvo un alto impacto el caso de Cambridge Analytica, empresa que aprovechó datos personales extraídos de la plataforma Facebook para influenciar y sesgar la opinión pública en procesos electorales.

A partir del año 2017, el Estado boliviano empezó la implementación del Plan de Gobierno Electrónico, para lo cual desarrolló nuevas herramientas y plataformas que requerían generar un tratamiento interoperable de datos entre diferentes entidades y sistemas informáticos. Consecuentemente, a partir de la Ley 1057, se estableció que el Servicio de Registro Cívico (SRECI) otorgue al Servicio General de Identificación Personal (SEGIP), acceso de consulta en línea mediante mecanismos de interoperabilidad, a todos los datos de certificados de nacimiento, estado civil y certificados de defunción de las personas naturales registradas en su base de datos. También habilitó servicios de verificación y contrastación en línea en tiempo real, de la información consignada en el registro biométrico. El mismo año, se promulgó la Ley de Ciudadanía digital (Ley 1080) con el objeto de establecer las condiciones y responsabilidades para el acceso pleno y ejercicio de la ciudadanía digital en el Estado Plurinacional de Bolivia.

3 <https://www.noticiasfides.com/nacional/sociedad/gualberto-cusi-paso-por-el-momento-mas-oscuro-pero-volvio-a-encontrarle-un-sentido-a-su-vida-365900-365806#:~:text=Ese%20lunes%20de%20diciembre,y%20en%20las%20redes%20sociales.>

Lo anterior, llevó a impulsar reflexiones sobre el acceso, uso y procesamiento de datos en grandes cantidades y de manera disruptiva con el uso de tecnología. El mismo año, en un conversatorio con periodistas con motivo del 17 de mayo, Día internacional de Internet, la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC) admitió públicamente “que Bolivia requiere una ley de protección de datos personales”. Esta afirmación permitió dar paso a la elaboración de un anteproyecto de ley⁴. Desde entonces, se trabaja en un proyecto a la ley que, casi ocho años después, aún no se concluye.

Desde ese entonces, se han visto mayores avances en el desarrollo de gobierno electrónico y digitalización del Estado, estableciéndose por ejemplo, el uso obligatorio del sistema de Ciudadanía Digital para facilitar los procesos de registros de datos y ser un mecanismo de autenticación de identidad. Así mismo, se registraron mayores abusos y situaciones de riesgo para los datos de la población.

El 2020, en época de pandemia, se emitieron los Decretos Supremos (D.S.) 4199⁵, 4200⁶ y 4231⁷, que habilitaban la posibilidad de denuncias penales en acciones de desinformación en el ámbito de salud. A pesar de ser derogados por el D.S. N° 4236, se registraron incidentes relacionados a su aplicación como la aprehensión de al menos 67 personas⁸ a partir de mecanismos de ciberpatrullaje. En 2021, fue aprehendido un Viceministro por la presunta utilización de datos de registros de identificación para persecución de contrincantes políticos⁹.

En 2023, el Estado boliviano inició la implementación de la cédula de identidad digital¹⁰ que consiste en un documento digital y portable en una aplicación móvil que cuenta con un sistema de autenticación con microchip. Al igual que en el caso de ciudadanía digital se observa el uso, almacenamiento y manejo de información sensible personal. Esto conlleva necesariamente a la mayor concentración de información que, en caso de robos de dispositivos, puede ser usada para actividades delictivas. Paralelamente en ese año, empezaron a implementarse tecnologías del reconocimiento facial en unidades educativas como política pública¹¹, poniendo en riesgo a una de las poblaciones más vulnerables: la niñez.

Además, el vacío de políticas públicas en la contención de amenazas y riesgos en materia de ciberseguridad es preocupante, con grandes indicios y sospechas de ingresos no autorizados a sistemas del Estado, en los cuales pudo haber exposición de datos personales. En 2022, una empresa internacional incluyó en su reporte que al menos 44 sistemas del Estado boliviano habían sido infiltrados, entre ellos Impuestos Nacionales,

4 <https://www.facebook.com/paginasiete/posts/agetic-admite-que-se-necesita-una-ley-de-proteccion-de-datos-del-director-de-la-ag-2016431521734577>

5 21 de marzo de 2020. <https://www.lexivox.org/norms/BO-DS-N4199.html>

6 25 de marzo de 2020. <https://www.lexivox.org/norms/BO-DS-N4200.html>

7 07 de mayo de 2020. <https://www.lexivox.org/norms/BO-DS-N4231.html>

8 Indicando que 37 ya tendrían condena porque se habrían encontrado los elementos suficientes y las personas se habrían acogido a procesos abreviados.

9 <https://erbol.com.bo/seguridad/aprehenden-guido-melgar-que-fue-vice-ministro-en-la-gesti%C3%B3n-de-a%C3%B1ez>

10 Riesgos de la cédula de identidad digital: <https://internetbolivia.org/nota-de-opinion/es-la-cedula-de-identidad-digital-necesaria/>

11 El uso indiscriminado de cámaras de reconocimiento facial en unidades educativas: <https://internetbolivia.org/nota-de-opinion/sonrie-te-estamos-filmando-el-riesgo-del-uso-de-reconocimiento-facial-en-escuelas/>

Ministerio de Educación, AGETIC y AEVivienda¹². Estos ingresos no autorizados daban la posibilidad de extraer estados de cuenta, datos personales, contraseñas, entre otros.

En 2024, el Observatorio de delitos informáticos de Bolivia ha denunciado en múltiples ocasiones, casos de venta de bases de datos en redes sociales con información personal de 12,5 millones de personas¹³. La información no fue confirmada y posteriormente el SEGIP¹⁴ alegó que los datos personales están protegidos y anunció una investigación¹⁵. Sin embargo, las denuncias y capturas de pantalla de la comercialización de esta información se han repetido en varias oportunidades. En julio de 2024, también denunciaron la posible vulneración al sistema de pasarela de pagos del Estado.

A la par de las sospechas de vulneraciones a sistemas gubernamentales y exposición de datos personales, también han aumentado considerablemente los casos de cibercrimen, varios de los cuales tienen una raíz en el uso de información de las personas. En los últimos años se han detectado una gran cantidad de robos bancarios virtuales que han implicado, por ejemplo, la posibilidad de que cibercriminales puedan saber al mismo tiempo números telefónicos, carnets de identidad, contraseñas y cuentas bancarias para poder acceder a la banca móvil de las personas¹⁶. Se registraron estafas virtuales a través de WhatsApp y otras herramientas de mensajería. Estas ciberestafas usan estrategias de ingeniería social para generar confianza en las personas, a través de no sólo saber sus números telefónicos pero también poder suplantar identidad de seres queridos¹⁷, para así lograr que estas hagan pagos o brinden información privada que luego es mal utilizada por los cibercriminales. En 2024 se pudo identificar un redes de cibercrimen que operaba de esa manera¹⁸. También se dieron casos con afectación directa a poblaciones vulnerables, como la divulgación sin consentimiento de la orientación sexual o la autoidentificación de género de personas para llevar adelante ataques a su reputación o promover discursos y crímenes de odio¹⁹, y el contacto no autorizado a adolescentes y niños y niñas por parte de adultos para delitos de grooming, explotación sexual y trata²⁰.

- 12 1. La brecha de ciberseguridad que podría haber afectado a 44 sitios del Gobierno: <https://internetbolivia.org/noticias/brecha-de-ciberseguridad-en-bolivia-nuestros-datos-están-protegidos/>
2. Durante el primer trimestre del 2024, se gestionaron 239 incidentes y vulnerabilidades, de acuerdo al Informe del Centro de Gestión de Incidentes Informáticos del Estado Plurinacional de Bolivia: <https://www.csirt.gob.bo/es/noticias/informe-de-gestion-de-incidentes-y-vulnerabilidades-informaticas-primer-trimestre-2024>
- 13 <https://x.com/GrupoFides/status/1795233530823262562?l=agf5ZG3LhiFeknoDnAeAw&s=0&https://odibolivia.org/2024/04/22/venta-de-base-de-datos-con-informacion-personal-de-12-5-millones-de-bolivianos/>
- 14 Servicio General de Identificación Personal.
- 15 <https://www.reduno.com.bo/noticias/segip-afirma-que-datos-personales-están-protegidos-y-anuncia-investigacion-tras-denuncias-de-venta-en-redes--2024527155650>
- 16 Casos de robos bancarios virtuales, realizados a través del uso no autorizado de datos personales para suplantar temporalmente líneas de celulares de las personas afectadas, y así, realizar retiros y transferencias de dinero: <https://dplnews.com/bolivia-robos-virtuales-así-apunta-a-clonaciones-y-el-bu-dice-que-sus-apps-son-seguras/>
<https://www.los tiempos.com/actualidad/economia/20211118/victimas-robo-virtual-suben-37-banco-union-promete-devolucion>
<https://www.opinion.com.bo/articulo/pais/así-advierte-que-denuncias-robo-virtual-banco-union-busca-corrída-depositos/20211019013305839656.html>
- 17 Una mujer reveló un elaborado esquema de estafa perpetrado por una red internacional compuesta por individuos coreanos y bolivianos: <https://www.reduno.com.bo/noticias/estafada-por-amor-doctora-creyo-encontrar-en-redes-a-su-media-naranja-y-le-robaron-bs-65-mil--2024531173111>
- 18 Denuncias sobre ciberestafas que realizan por medio de WhatsApp con el hackeo de cuentas: <https://www.reduno.com.bo/noticias/no-desconfie-y-le-transferi-hackearon-el-whatsapp-de-su-amiga-y-la-estafaron-con-bs-2-mil-2024522161223>
- 19 La FELCC ejecutó un operativo para la aprehensión de miembros de una empresa presuntamente dedicada al cibercrimen: <https://www.reduno.com.bo/noticias/117-aprehendidos-en-operativo-contra-cuartel-de-ciberestafadores-en-santa-cruz-202452911180>
- 20 Publicación no autorizada de datos personales obtenidos en Grindr: Pg. 11 <https://internetbolivia.org/wp-content/uploads/2023/08/Advancing-Data-Justice-Research-and-Practice-Final-Report-Internet-Bolivia.pdf>
- 20 <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.opinion.com.bo/articulo/policial/nina-contactada-redes-sociales-sufre-abuso-sexual-quillacollo/2023112800048928842.html&ved=2ahUKEwjJkS2veqHAXHqJUCHc4zHUIQfnoECB0QAO&usq=AOWwaw268DP2cJn-yjEP9K41sG0H>

También se empezó a observar una mayor comercialización de bases de datos con fines comerciales, de marketing o financieros o el análisis de riesgos por parte de seguros, lo cual aumenta de manera exorbitante y constante en Bolivia. Es así que es importante analizar cómo se están desarrollando y aplicando las tecnologías INSURTECH²¹, REGTECH²², FINTECH²³, entre otras. El uso y comercialización de bases de datos es evidente, ya que se observa este tipo de accionar en redes como Facebook – Marketplace.

Todas las anteriores situaciones son propias de un contexto de mayor digitalización, sin embargo, la ausencia de marcos normativos de protección, incrementa sus niveles de afectación y reduce considerablemente los márgenes de acción y respuesta por parte de autoridades.

LA PROTECCIÓN DE DATOS COMO DERECHO HUMANO

El tratamiento inadecuado de los datos, y/o sin las medidas necesarias de seguridad, puede dar lugar a varios tipos de abusos que ya fueron mencionados, que colocan a las personas en una alta situación de vulnerabilidad ante violencias digitales y ciberdelitos, mal registro y uso de su información, que pueden perjudicar en sus trámites, procesos judiciales u otros, entre otras situaciones.

Bolivia es firmante y adherente de múltiples instrumentos internacionales que son parte del sistema de protección de derechos humanos como ser: Declaración Universal de Derechos Humanos, Convención Internacional de Derechos Civiles y Políticos, Convención Internacional para la Eliminación de todas las Formas de Discriminación contra la Mujer y Pacto Internacional de Derechos Económicos, Sociales y Culturales. Así también, al ser parte de la Organización de Estados Americanos, se adhirió a la Convención Americana de Derechos Humanos.

Es necesario mencionar que en el año 2024, Bolivia se adhirió al MERCOSUR, lo que lleva al país a replantear su posición para implementar una normativa referente a la protección de datos personales. El MERCOSUR fue desarrollando y trabajando, el Tratado de Asunción, Protocolo de Ouro Preto y la Decisión 15/20 referente al Acuerdo sobre Comercio Electrónico, que establece derechos mínimos que deben garantizar los Países Miembros, adoptando o manteniendo leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios, con el objetivo de mejorar la confianza que tienen los consumidores en el comercio electrónico.

²¹ INSURTECH, se refiere al uso de tecnología innovadora en la industria de los seguros, su objetivo es optimizar la eficiencia, reducir costos y ofrecer productos más personalizados.

²² REGTECH, describe el uso de tecnología para ayudar a las empresas a cumplir con las regulaciones legales y normativas, principalmente en el sector financiero. Las soluciones que brinda se enfocan en automatizar y agilizar procesos de cumplimiento normativo, incluyendo el monitoreo de transacciones, la detección de fraude y la presentación de informes regulatorios.

²³ FINTECH, es un término más amplio que abarca a las empresas y plataformas tecnológicas que brindan servicios financieros innovadores, incluye una variedad de servicios como pagos móviles, préstamos en línea, criptomonedas, gestión de inversiones y banca digital.

Por otro lado, se encuentran las diferentes propuestas de implementación como la Decisión MERCOSUR/CMC/P. DEC. N° 10, donde se determina que los Estados partes deben incorporar la presente Decisión a sus ordenamientos jurídicos nacionales, la cual tiene como objeto que “la protección integral de los datos de las personas físicas asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados que excedan el uso exclusivo personal, para garantizar el derecho al honor y la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre”.

LEGISLACIÓN EXISTENTE

Es necesario mencionar que hasta el año 2009 se contaba con la figura del *Habeas Data* y con la reforma de la Constitución vemos que se comienza a emplear la figura “Acción de protección de privacidad”.

Entonces, si bien no se cuenta con una ley de protección de datos existen ciertos articulados que se fueron adecuando a las nuevas necesidades planteadas. A continuación se los detalla.

Constitución Política del Estado

- ARTÍCULO 130.- “... I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.”
- ARTÍCULO 131.- “... I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional. II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución. IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.”

Código Civil

- ARTÍCULO 12. (PROTECCIÓN DEL NOMBRE).- “...La persona a quien se discuta el derecho al nombre que lleva o sufra algún perjuicio por el uso indebido que de ese nombre haga otra persona, puede pedir judicialmente el reconocimiento de su derecho o la cesación del uso lesivo . El juez puede ordenar que la sentencia se publique por la prensa.”
- ARTÍCULO 16. (DERECHO A LA IMAGEN).- “... I. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo. II. Se comprende en la regla anterior la reproducción de la voz de una persona”
- ARTÍCULO 17. (DERECHO AL HONOR).- “... Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes”
- ARTÍCULO 18. (DERECHO A LA INTIMIDAD).- “...Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley”
- ARTÍCULO 19. (INVIOLABILIDAD DE LAS COMUNICACIONES Y PAPELES PRIVADOS).- “... I. Las comunicaciones, la correspondencia epistolar y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente. II. No surten ningún efecto legal las cartas y otros papeles privados que han sido violados o sustraídos, ni las grabaciones clandestinas de conversaciones o comunicaciones privadas”

NECESIDADES Y ARGUMENTOS PARA UNA LEY DE PROTECCIÓN DE DATOS PERSONALES

Si bien hay avances en esta materia, es preciso poder contar con una normativa específica que incluya y avance la protección de datos personales en razón a los siguientes necesidades y argumentos:

- **Introducción al consentimiento informado como condición para el tratamiento de datos:**

En los últimos años, el consentimiento informado comenzó a desarrollarse en temas de privacidad y protección de datos, ya que diferentes plataformas, así como empresas y organizaciones en general, en muchos casos vulneran datos personales haciendo mención al consentimiento. Sin embargo, cuando se consultaba a los usuarios sobre el consentimiento vertido a un acuerdo o términos y condiciones de uso, el usuario no estaba realmente al tanto de lo que había aceptado. Por lo cual no es lo mismo la implementación del consentimiento en cualquier reglamento o términos y condiciones de uso, que un consentimiento informado, donde el usuario, usuaria, ciudadana o ciudadano sea consciente del alcance de la aceptación. Todo esto en busca del uso del consentimiento como herramienta para el resguardo de Derechos Digitales y no como un arma hacia quien lo da.

- **Inclusión de los denominados derechos ARCO:**

Con el desarrollo de normativas referentes a protección de Derechos Digitales y protección de la Privacidad, se comenzó a trabajar en los denominados Derechos ARCO, que como sus siglas definen, buscan definir ciertos Derechos sobre nuestros datos, como ser el Acceso, Rectificación, Cancelación y Oposición. Sin embargo, con el tiempo se observaron otros inherentes a nuestros datos, como ser Derecho sobre la portabilidad de datos, limitación de tratamiento, decisiones automatizadas y perfilado de datos, Derecho al olvido, seguridad de datos y en los últimos años, el consentimiento informado como derecho inherente a los datos personales.

- **Facilitar los procesos administrativos:**

Las herramientas y derechos necesarios para garantizar la protección de datos personales va de la mano de la existencia de procedimientos judiciales y administrativos que permitan a las personas, de manera fácil y rápida, hacer valer sus derechos ante entidades públicas y/o privadas. Sin embargo, en el caso de Bolivia, existe sólo la posibilidad de invocar la “autodeterminación informativa” sólo a través de mecanismos judiciales, los cuales pueden ser lentos, costosos y difíciles de aplicar.

Dentro de las garantías constitucionales y los procesos en general, se menciona el agotar vías administrativas antes de llegar a estrados judiciales, aunque en temas de protección de datos y privacidad, las y los ciudadanos no suelen agotar estas vías, convirtiendo procesos que podrían ser más rápidos en procesos largos y en muchos casos poco eficientes.

Además de ser erróneo este camino, la protección de datos y privacidad requiere de cierta celeridad, ya que la vulneración de uno o varios datos personales, puede ser la puerta de entrada para vulnerar otros derechos y libertades.

En ese sentido, la existencia de una ley de protección de datos ayudaría a reducir tiempos de procesos administrativos, para el acceso, rectificación, cancelación u oposición de datos que pueden tener un registro erróneo o que causa algún tipo de perjuicio a una determinada persona al ser inexactos o no estar actualizados, evitando procesos que significan un costo de recursos económicos, así como tiempo y en ciertos casos consecuencias psicológicas, por lo desgastante y largo que resultan este tipo de trámites.

- **No ser sujeto a decisiones automatizadas:**

En el año 2018 se comienza a hablar sobre privacidad y los derechos de las y los usuarios sobre sus datos, privacidad e intimidad, y el derecho sobre las decisiones automatizadas y perfilado de datos, que en ese momento, era un derecho poco ejercido. Con el desarrollo del Big Data, Machine Learning, IoT (Internet de las cosas), la Inteligencia Artificial y otras tecnologías emergentes las decisiones automatizadas y perfilado de datos, se convirtieron en algo del día a día, que resulta ser riesgoso, ya que los datos almacenados y procesados pueden estar sujetos a sesgos algorítmicos que pueden mostrar resultados poco reales o un bajo nivel de comprobación.

Las respuestas inexactas de datos, es solamente uno de los problemas que se identifican en el análisis de grandes cantidades de datos, para el proceso de modelaje de inteligencia artificial, el problema es que estas tecnologías requieren de datos para funcionar y las bases de recolección de datos son las usuarias y los usuarios. No es coincidencia que se mencione a los datos como el petróleo de este siglo, ya que sin datos ninguna Inteligencia Artificial podría funcionar.

Es urgente trabajar en una ley de protección de datos que permita fijar lineamientos para el uso de la Inteligencia Artificial de manera ética.

ACCIONES IMPULSADAS PARA LOGRAR LA PROTECCIÓN DE DATOS DESDE SOCIEDAD CIVIL

Desde el año 2018, la Fundación InternetBolivia.org comenzó con la concientización y difusión de información sobre la protección de datos personales, buscando la aprobación de una ley que garantice los derechos de la ciudadanía.

En 2019, luego de tres eventos en las ciudades de La Paz, Santa Cruz y Cochabamba, se presentó en mayo de ese año un primer anteproyecto de ley ante la Asamblea Legislativa²⁴. Esta propuesta, a raíz de los eventos políticos de ese entonces, no llegó a ser discutida pero quedó como un antecedente positivo en la temática. Posterior a la pandemia, en 2021, la Fundación InternetBolivia.org retomó su campaña y esfuerzos en este proceso.

Entre 2021 y 2023, se llevaron adelante talleres en al menos 10 ciudades de Bolivia (Sucre, El Alto, La Paz, Cochabamba, Santa Cruz, Tarija, Oruro, Coroico, Copacabana y Villamontes) y 30 reuniones con distintos actores estratégicos públicos y privados incluidos: CAINCO, Cámara Nacional de Comercio, Universidad Misael Saracho, Universidad San Francisco Xavier, Universidad Católica Boliviana, Universidad Pública de El Alto, UDABOL, Capítulo ISOC Bolivia, Municipio de Coroico, Gobernación de Chuquisaca, entre otros.

El resultado de estas actividades, fue un nuevo anteproyecto de ley de protección de datos que fue reforzado con más de 200 comentarios de diferentes actores.

Paralelamente, en esos años también se trabajó de cerca con el Gobierno Autónomo Municipal de Coroico, así como varias organizaciones sociales de base de ese municipio, federaciones de productores campesinos, juntas de padres y madres de familia, entre otros. A partir de ello, la Fundación InternetBolivia.org y la Asociación Aguayo, lograron que en 2023 el Concejo Municipal de Coroico apruebe la “Ley municipal de digitalización y gestión de datos”²⁵. Esta normativa avanzaba el desarrollo de un gobierno electrónico, pero incluía aspectos de privacidad y protección de datos personales, desde el mismo diseño y propuesta de implementación basándose en estándares internacionales. Se incluía en esta:

- Mejora de servicios con un tratamiento de datos de manera adecuada.
- Ser soporte en el proceso de digitalización de datos.
- Concientización a funcionarios y a ciudadanos sobre la importancia de la protección de datos.
- Tratamiento adecuado de la base municipal de datos personales a través de la unidad administrativa.
- Educación tecnológica para la protección de datos personales.

²⁴ <https://www.informatica-juridica.com/anteproyecto-de-ley/anteproyecto-de-ley-proteccion-de-datos-personales-mayo-2019/>

²⁵ <https://internetbolivia.org/actividades/comunicados/coroico-primer-municipio-de-bolivia-con-regulacion-de-proteccion-de-datos/>

El proceso de aprobación incluyó una metodología de trabajo basada en el activismo y la participación abierta, con el uso de obras de teatro, muralismo y talleres de alfabetización digital para generar concientización sobre los derechos digitales. Por estas razones, la ley de Coroico se convirtió en un hito pues implicó la primera iniciativa de esa índole en Bolivia. Posteriormente, se trabajó en una reglamentación y se realizaron diversas acciones para empezar su implementación, como capacitaciones y talleres para los funcionarios públicos²⁶.

Entre 2023 y 2024, se logró generar una red de actores de sociedad civil que están haciendo seguimiento a la temática, la cual está compuesta por organizaciones como Wikimedistas de Bolivia, ADESPROC Libertad, HCS Abogados, Save the Children, Plataforma STATUS, Fundación InternetBolivia.org e investigadores que se sumaron a título individual.

DESDE EL ESTADO

El Gobierno boliviano, a partir de la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), asumió la necesidad de contar con una ley de protección de datos personales desde el año 2018²⁷. Desde entonces, ha estado trabajando en un anteproyecto, desarrollado en diferentes etapas.

Entre 2018 y 2019, la AGETIC contrató a especialistas nacionales para llevar adelante talleres participativos para entender las necesidades en la temática y elaborar posteriormente un anteproyecto que por diversos motivos no llegó a concretarse. En 2022, reinició este proceso con apoyo de organismos internacionales y en noviembre de ese año, presentó una primera versión de su propuesta a especialistas y miembros de la sociedad civil. En 2023, realizó una serie de jornadas públicas para socializar su anteproyecto con el apoyo de un consultor internacional, quién estuvo a cargo de desarrollar el documento.²⁸ Esta presentación estuvo acompañada de solicitudes para mandar contribuciones, motivo por el cual, la Fundación InternetBolivia.org, junto a las organizaciones bolivianas Asociación Civil de Desarrollo Social y Promoción Cultural Libertad (ADESPROC – Libertad) y Wikimedistas de Bolivia y la organización internacional Access Now, analizaron el documento compartido por AGETIC para hacer aportes y sugerencias con el afán de fortalecer la perspectiva garantista de Derechos Humanos, haciendo sugerencias en al menos 18 artículos²⁹.

Hasta finales de 2024, el único avance tangible en materia de protección de datos sigue siendo la “Ley Municipal de Digitalización y Gestión de Datos” que fue aprobada e implementada por el Municipio de Coroico.

²⁶ <https://internetbolivia.org/nota-de-prensa/coroico-inicia-la-reglamentacion-de-su-ley-de-digitalizacion-y-gestion-de-datos/>

²⁷ <https://www.facebook.com/paginasiete/posts/agetic-admite-que-se-necesita-una-ley-de-proteccion-de-datos-el-director-de-la-ag/2016431521734577/>

²⁸ <https://www.agetic.gob.bo/la-agetic-lleva-a-cabo-la-socializacion-del-anteproyecto-de-ley-de-proteccion-de-datos-personales/>

²⁹ <https://internetbolivia.org/actividades/comunicados/hacia-una-ley-de-proteccion-de-datos-personales-que-garantice-nuestros-derechos/>

HACIA LA CONSTRUCCIÓN DE PROPUESTAS ELECTORALES

Dado el contexto electoral 2024-2025 y la oportunidad que abre la Ley de Organizaciones Políticas - Ley 1096 -, la cual en sus Artículos 20 y 21 establece la formulación de plataformas programáticas y propuestas de gobierno desde las organizaciones y partidos políticos, se organizó un taller el 4 de septiembre del año 2024, con activistas y miembros de organizaciones políticas para construir escenarios prospectivos y pre-propuestas electorales en la agenda de derechos digitales en Bolivia³⁰.

Este espacio posibilitó la participación de un grupo plural de 30 personas, 45% de las cuales se identificaba con una organización política y 42% con colectivos o plataformas activistas de diversa índole (derechos humanos, derechos de las mujeres, participación de jóvenes, LGTBIQ+, entre otros). Se convocó a este grupo con el objetivo de evaluar y validar la importancia de la agenda de temas de tecnología y digitalización en los próximos procesos electorales: judicial, general y subnacional, identificar patrones y temáticas de relevancia, y finalmente, construir en grupos temáticos, bases de posibles propuestas electorales.

Desde una perspectiva general, para los y las participantes del espacio, se identificó a las tecnologías digitales como una temática prioritaria y determinante para el debate electoral 2025-2026. El contexto de recesión económica y percepción de condiciones más adversas para el “bolsillo de la ciudadanía” es tomado como la temática que genera más preocupación. No obstante, se mencionó que aquellos candidatos/as que centren sus propuestas en soluciones a esta situación, en las cuales se resalte el rol de la digitalización para impulsar nuevos emprendimientos, capacidades y oportunidades para la población, podrían tener una mayor opción de interesar a los y las votantes más indecisas - que son aquellas que son más susceptibles de ser convencidas por la propuestas programáticas más que por las convicciones políticas y/o ideológicas.

La percepción de los y las participantes sobre cuál determinante será la agenda digital al momento de decidir la votación, tuvo una alta valoración: 39% de ellos y ellas indicaron que será “muy determinante” y 42% que será “relativamente determinante” (Gráfico 1). De hecho, al dividir la pregunta por sectores específicos, resaltó que la valoración positiva será aún más en la población joven, en tanto los y las participantes indicaron que será muy determinante para alrededor del 59%, y podría serlo también para los padres, madres y tutores - en relación al bienestar de sus hijos e hijas - 44%.

³⁰ Evento realizado el 5 de septiembre de 2024 en la ciudad de La Paz.

Gráfico 1. Percepción de las y los participantes sobre cuán determinante son los temas para captar votos de la población en general

Si la respuesta anterior es sí o parcialmente

¿Qué tan determinante sería para captar votos de la población en general?

31 Respuestas

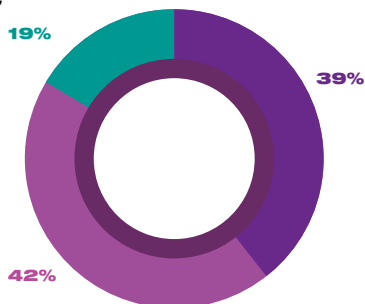
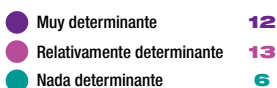


Gráfico 2. Percepción de las y los participantes sobre cuán determinante son los temas para captar votos de la población joven

¿Qué tan determinante sería para captar votos de la población joven?

32 Respuestas

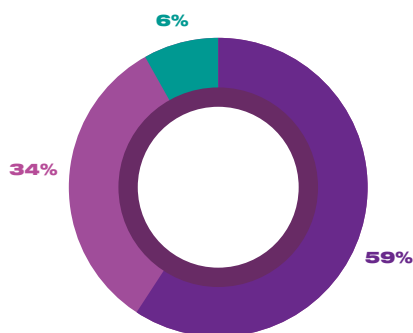
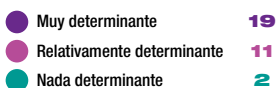
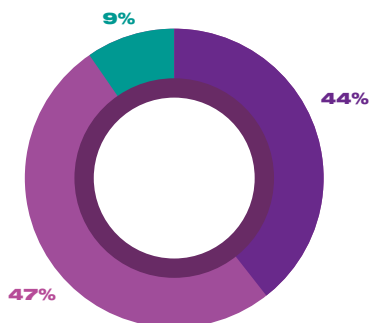
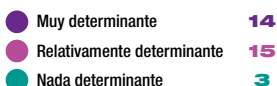


Gráfico 3. Percepción de las y los participantes sobre cuán determinante son los temas para captar votos de los padres, madres y/o tutores

¿Qué tan determinante sería para captar votos de padres/madres de familia o tutores preocupados para la vulneración de derechos a sus hijos/as/es?

32 Respuestas



A nivel individual, se sondeó con los y las participantes sobre cuáles consideran serán los temas más relevantes con respecto a la digitalización en Bolivia. Las respuestas revelaron que los problemas más destacados y que generan interés son: acceso a la tecnología/internet, desarrollo e impulso de la economía digital, manejo de la información y protección de datos, y lucha contra la violencia en línea.

Tabla 1. Grupo de temáticas de la agenda de derechos digitales que requieren de política pública (identificados por clusters)

LIBERTAD DE EXPRESIÓN Y DESINFORMACIÓN	VIOLENCIAS DIGITALES	INCLUSIÓN Y ACCESO A INTERNET	PRIVACIDAD, DATOS PERSONALES E INTELIGENCIA ARTIFICIAL
Aprobación de una ley de protección de datos personales	Diseño de una política integral de lucha contra las violencias digitales	Agenda digital para cierre brecha digital	Programa de economía de desarrollo económico basado en la transformación digital y de datos
Fortalecimiento del gobierno digital		Incremento de la inversión público-privada para la infraestructura digital	Eficiencia institucional y soberanía digital
Ley de acceso a la información y manejo de datos abiertos		Programas masivos de educación en habilidades digitales	Ley de protección de datos personales
		Impulsar una visión consciente entre digitalización y medio ambiente	Ciberseguridad

Si bien los temas son aún generales y requieren un trabajo a profundidad con actores sociales y políticos, es positivo que representantes de partidos y organizaciones que se lanzarán en las próximas campañas, incluyan en sus posibles propuestas acciones específicas para fortalecer los derechos humanos en entornos digitales. Aunque esta sólo fue una aproximación, dio suficientes insumos para construir una base de pre-propuestas que serán desarrolladas en siguientes espacios de reflexión.

A partir de las perspectivas antes descritas y dialogadas en los grupos de trabajo, y sobre la base de lo avanzado por el sector público y la sociedad civil, se derivó en la construcción de pre-propuestas electorales en dos marcos: económico y gobierno digital.

PROPUESTAS EN EL ENTORNO ECONÓMICO:

- Los datos son actualmente un insumo importante para impulsar la economía digital. Su uso efectivo facilita la toma de decisiones a distintos niveles, el entrenamiento de modelos de Inteligencia Artificial, el desarrollo de nuevas herramientas y servicios para la planificación geográfica, la agroindustria, la gestión urbana, entre otros. Sin embargo, no se puede avanzar en estos sin tener acceso a información de calidad y mecanismos claros que resguarden los datos personales. Por ello, es necesario establecer un marco jurídico que habilite a ambos procesos, a través de una **ley de acceso a información y datos abiertos, así como una ley de protección de datos personales**.
- Se puede impulsar la **generación de lineamientos claros para empresas privadas con respecto a la protección de datos que respeten los estándares internacionales**. Esto les permitirá ser competitivas a nivel internacional y poder ser parte de licitaciones en otros países, ofrecer servicios a ciudadanos/as extranjeros, entrar en mecanismos de outsourcing, entre otros negocios digitales.
- Es necesario avanzar en el desarrollo de un **entorno habilitante propositivo con los derechos la privacidad, la protección de datos y la información**, a través de un marco regulatorio estandarizado a nivel internacional en temas de protección de datos personales y seguridad de la información, para que empresas tecnológicas internacionales puedan invertir en Bolivia con mayor facilidad.
- El adecuado aprovechamiento de las tecnologías de Inteligencia Artificial son hoy considerados determinantes para dar grandes saltos a nivel de la eficiencia y productividad de todos los sectores económicos. Su uso puede ser de un gran beneficio para la población. Sin embargo, se debe considerar generar las capacidades y habilidades digitales necesarias en la ciudadanía, así como implementar los resguardos necesarios para el uso seguro y ético de éstas. Por ello, se propone **la realización de un estudio exploratorio que identifique los sectores que puedan ser más beneficiados por las Inteligencias Artificiales, la adaptación de un marco regulatorio que reduzca los riesgos de su implementación y generar programas de nivelación y desarrollo de capacidades desde un enfoque productivo**.

PROPUESTAS EN GOBIERNO DIGITAL:

- **El gobierno abierto y sus mecanismos de transparencia y rendición de cuentas son herramientas necesarias para salvaguardar el adecuado uso de la información** por parte de actores públicos y privados. Por ello, Bolivia debe adoptar un marco comprensivo que permita control social sobre el manejo de los datos personales de los bolivianos y bolivianas.
- **Las competencias de seguimiento del cumplimiento de la protección de datos y el acceso a información no pueden estar sujetas a las decisiones e intereses del Gobierno ejecutivo**, por que entonces, pierden su capacidad de control social. Por ello, el Estado boliviano debe crear una entidad competente e independiente con la capacidad de hacer cumplir que los derechos digitales de los bolivianos y las bolivianas se protejan.
- **La interoperabilidad de datos es un paso necesario para generar eficiencia institucional.** Se debe priorizar la adopción de una regulación nacional que incluya tanto mecanismos técnicos y legales que incluyan salvaguardas de derechos humanos para garantizar el adecuado uso de la información.
- Se requiere **fortalecer la capacidad de gestión de la ciberseguridad y la seguridad de la información por parte del Estado boliviano.** Es necesario avanzar en generar una política a nivel nacional que establezca los lineamientos técnicos para todo el aparato público y que colabore con el sector privado. Asimismo, se debe crear una agencia de ciberseguridad especializada que brinde institucionalización, seguridad y confianza en la protección de todos los activos digitales y de información del Estado.
- Se propone la **creación de una oficina o secretaria especializada en impulsar el uso estratégico de las Inteligencias Artificiales** en los procesos burocráticos del Estado, su aprovechamiento en la educación y la economía, que genere nexos y trabaje en asocio con el sector privado, las universidades y la sociedad civil especializada. Esta debe velar por un uso ético y responsable de las IA desde un marco de derechos humanos.
- **La reforma judicial pendiente en Bolivia debe incluir una mirada desde la innovación tecnológica, remarcando la modernización de los procesos jurídicos y de toma de decisiones**, los mecanismos de justicia abierta y transparente, la inclusión de los derechos digitales - incluyendo la protección de datos personales, la privacidad, el acceso a información, la integridad informacional -, y su actualización con respecto a los ciberdelitos.