



ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS



La Paz, 23 de marzo de 2026  
CDH/NI N° 99/2025-2026

Señor:  
Roberto Julio Castro Salazar  
**PRESIDENTE**  
**CÁMARA DE DIPUTADOS**  
Presente. -



**REF.: PRESENTA PROYECTO DE LEY**

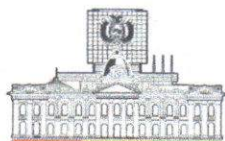
De mi mayor consideración:

A tiempo de saludarle y deseándole éxito en las funciones que desempeña, mediante la presente, de conformidad a lo establecido por el numeral 2, párrafo I del Artículo 162 de la Constitución Política del Estado, concordante con el inciso b del Artículo 116 y Artículo 117 del Reglamento General de la Cámara de Diputados, tengo a bien presentar el **“PROYECTO DE LEY INTEGRAL CONTRA LA VIOLENCIA DIGITAL”** para su tratamiento legislativo correspondiente conforme a normativa.

Sin otro particular y seguro de que la presente será merecedora de su gentil atención, me despido con las consideraciones más distinguidas.

  
Abog. W. Marcelo Solís Valencia  
DIPUTADO NACIONAL  
CH'QUISACA  
ASAMBLEA LEGISLATIVA PLURINACIONAL

C.C. ARCH. WMSV  
Contacto: 60115718



• CÁMARA DE DIPUTADOS •  
2025-2026

¡QUE DIOS ILUMINE NUESTROS PASOS Y QUE EL PUEBLO JUZGUE NUESTRO TRABAJO!



ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

CÁMARA DE DIPUTADOS  
A LA COMISIÓN DE  
DERECHOS HUMANOS  
SECRETARÍA GENERAL

## PROYECTO DE LEY INTEGRAL CONTRA LA VIOLENCIA DIGITAL

### EXPOSICIÓN DE MOTIVOS

#### 1. ANTECEDENTES

El acelerado desarrollo de las tecnologías de la información y comunicación ha transformado profundamente las formas de interacción social, política, económica y cultural. Internet, las redes sociales, las plataformas digitales y los servicios de mensajería constituyen hoy espacios fundamentales para el ejercicio de derechos como la libertad de expresión, el acceso a la información, la participación política, la educación, el trabajo y la organización social.

No obstante, estos mismos entornos han sido utilizados para reproducir, amplificar y sofisticar diversas formas de violencia, discriminación y abuso, afectando la dignidad, la seguridad, la privacidad y la participación de las personas.

En este contexto, se ha evidenciado un incremento sostenido de conductas como el acoso digital, la difusión no consentida de contenido íntimo, la suplantación de identidad, la extorsión sexual digital, la difusión maliciosa de datos personales, así como la manipulación de imágenes mediante tecnologías emergentes — incluyendo inteligencia artificial— con fines de violencia sexual o reputacional.

Estas conductas generan impactos graves y multidimensionales en las víctimas, afectando su salud mental, su integridad personal, su seguridad, su reputación, su autonomía y su participación en la vida pública y digital. En consecuencia, la violencia digital no puede ser considerada como un fenómeno menor o "virtual", sino como una manifestación real y concreta de violencia con efectos tangibles en la vida de las personas.

En el contexto boliviano, este fenómeno adquiere especial relevancia debido al creciente acceso a internet y a dispositivos móviles en todo el territorio nacional, lo que ha ampliado el alcance de estas conductas sin que exista, en paralelo, un desarrollo normativo específico y suficientemente robusto que permita su abordaje integral.

#### 2. MARCO NORMATIVO Y AVANCES

La violencia digital constituye una extensión de las desigualdades estructurales de la sociedad, particularmente de aquellas basadas en género. Diversos estudios evidencian que las mujeres, niñas y adolescentes, así como periodistas, defensoras de derechos humanos, líderes sociales y personas con alta visibilidad pública, enfrentan una exposición desproporcionada a estas formas de violencia.

El Estado boliviano tiene la obligación de prevenir, investigar, sancionar y reparar todas las formas de violencia, conforme a la Constitución Política del Estado, que reconoce de manera expresa el derecho a la dignidad, la integridad física, psicológica y sexual, la igualdad y la no discriminación, así como el derecho a una vida libre de violencia, particularmente en sus artículos 14, 15 y 21.



• CÁMARA DE DIPUTADOS •

2025-2026



ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

Asimismo, la Constitución establece el derecho a la privacidad, la honra y la propia imagen, así como la inviolabilidad de las comunicaciones privadas, derechos que adquieren una dimensión específica en los entornos digitales y que requieren protección efectiva frente a nuevas formas de vulneración tecnológica.

El bloque de constitucionalidad, integrado por los tratados internacionales de derechos humanos ratificados por el Estado boliviano, refuerza estas obligaciones. En particular, la Convención Americana sobre Derechos Humanos y la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará) establecen el deber de los Estados de adoptar medidas legislativas, administrativas y judiciales para garantizar una vida libre de violencia, incluyendo aquellas manifestaciones que se producen en entornos digitales o mediados por tecnologías.

En el ámbito interno, si bien existen avances normativos relevantes, estos resultan insuficientes frente a la complejidad de la violencia digital. La Ley N° 348 (Ley Integral para Garantizar a las Mujeres una Vida Libre de Violencia) reconoce diversas formas de violencia, pero no desarrolla de manera específica las conductas que se producen en entornos digitales ni establece mecanismos adecuados de respuesta frente a ellas.

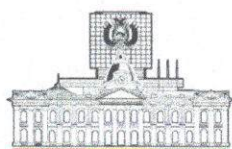
Por su parte, la Ley N° 548 (Código Niña, Niño y Adolescente) contempla la protección frente a riesgos en entornos tecnológicos, pero carece de herramientas específicas para abordar fenómenos como la sextorsión, el grooming digital o la difusión no consentida de contenido íntimo.

Asimismo, la Ley N° 263 (Ley Integral contra la Trata y Tráfico de Personas) incluye disposiciones relacionadas con el uso de medios tecnológicos para la comisión de delitos, pero su alcance es limitado y no cubre el conjunto de manifestaciones de la violencia digital.

Adicionalmente, el ordenamiento penal vigente no tipifica de manera clara y específica varias de estas conductas, lo que genera vacíos legales, dificultades probatorias y barreras de acceso a la justicia para las víctimas.

A nivel regional, se han producido avances significativos. La denominada "Ley Olimpia" en México marcó un hito en el reconocimiento de la violencia digital como una forma específica de violencia de género, impulsando reformas legislativas en diversos países de América Latina. Asimismo, el Comité de Expertas del Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) ha desarrollado la Ley Modelo Interamericana sobre Violencia Digital contra las Mujeres, que establece estándares para la prevención, sanción y erradicación de estas conductas.

En Bolivia, organizaciones de la sociedad civil, colectivos de víctimas y redes de acompañamiento han desempeñado un rol fundamental en la visibilización de esta problemática, destacando la necesidad urgente de contar con una normativa integral. En este marco, el movimiento articulado en torno a la Ley Olimpia Bolivia ha impulsado propuestas normativas orientadas a cerrar estos vacíos y garantizar una protección efectiva de los derechos en entornos digitales.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

### 3. ESTADO DE SITUACIÓN DE LA VIOLENCIA DIGITAL

La evidencia empírica confirma la magnitud y gravedad de la violencia digital en Bolivia y la región.

El diagnóstico “La violencia que no se ve, pero se siente” establece que la violencia digital no es virtual en sus efectos, sino que produce consecuencias reales y profundas en la vida de las personas.

El estudio “Palabras que Atacan” del Programa de las Naciones Unidas para el Desarrollo (PNUD, 2025) señala que, en países de la región como Bolivia, hasta el 40% de las interacciones en redes sociales dirigidas a mujeres en espacios públicos —como políticas y periodistas— contienen componentes de violencia digital.

Por su parte, la Encuesta Nacional Conectando Bolivia (AGETIC, 2025) evidencia que:

- i. El 31% de las mujeres ha sufrido abuso de sus datos personales, y
- ii. El 27% ha sido víctima de abuso sexual vinculado al uso de tecnologías, incluyendo sextorsión y difusión no consentida de contenido íntimo.

Asimismo, datos de ONU Mujeres Bolivia (2025) confirman que la violencia digital afecta de manera desproporcionada a mujeres jóvenes y adolescentes, quienes constituyen uno de los grupos más expuestos a este tipo de agresiones.

A nivel regional, se ha identificado que la violencia digital reproduce patrones estructurales de desigualdad de género. En este sentido, datos comparados indican que una proporción significativa de agresores identificados por víctimas son hombres, lo que evidencia la persistencia de relaciones de poder desiguales también en el entorno digital.

De igual manera, la expansión de tecnologías emergentes ha intensificado nuevas formas de violencia. Según ONU Mujeres (2025), aproximadamente el 95% de los contenidos “deepfake” de carácter sexual en internet tienen como víctimas a mujeres, siendo utilizados para extorsión, acoso o daño reputacional.

Los impactos de esta violencia son severos. Estudios regionales señalan que hasta el 70% de las víctimas de violencia digital experimentan acoso reiterado, lo que genera efectos como ansiedad, depresión y el denominado “silenciamiento digital”, consistente en la retirada o autoexclusión de los espacios digitales por temor a nuevas agresiones.

En el caso boliviano, estos efectos se ven agravados por limitaciones estructurales en el acceso a mecanismos de denuncia, la falta de especialización institucional en delitos tecnológicos, la limitada alfabetización digital en ciertos sectores de la población y la ausencia de protocolos claros de actuación para autoridades policiales, fiscales y judiciales.

Pese a esta realidad, Bolivia enfrenta un importante subregistro, debido a la ausencia de sistemas oficiales específicos de recolección de datos sobre violencia digital, lo que limita la formulación de políticas públicas efectivas y evidencia la





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

necesidad de un marco normativo que permita visibilizar, prevenir y sancionar estas conductas.

#### 4. OBJETO DEL PROYECTO DE LEY

La presente Ley tiene por objeto establecer un marco normativo integral para la prevención, atención, protección, investigación, sanción y reparación de la violencia digital, garantizando el ejercicio pleno de los derechos fundamentales en entornos digitales.

Asimismo, la Ley busca fortalecer las capacidades institucionales del Estado, promover la coordinación interinstitucional y establecer obligaciones diferenciadas para los distintos actores involucrados, incluyendo intermediarios de internet y plataformas digitales, en el marco de estándares de debida diligencia, responsabilidad ulterior y cooperación con autoridades competentes.

De igual forma, se pretende incorporar un enfoque preventivo y educativo, promoviendo la alfabetización digital, la cultura de respeto en entornos virtuales y el uso seguro de tecnologías, especialmente en poblaciones en situación de vulnerabilidad.

La norma también busca garantizar mecanismos eficaces de protección a las víctimas, incluyendo medidas de respuesta rápida, eliminación de contenidos lesivos, resguardo de pruebas digitales y atención integral.

De manera transversal, la Ley reconoce la centralidad del derecho a la libertad de expresión y prohíbe toda forma de censura previa. En consecuencia, las medidas que se adopten deberán aplicarse conforme a los principios de legalidad, necesidad y proporcionalidad, en concordancia con la Constitución Política del Estado y los estándares del derecho internacional de los derechos humanos, asegurando un equilibrio adecuado entre la protección de derechos y la preservación de un entorno digital libre y democrático.

  
Abog. W. Marcelo Solís Valencia  
DIPUTADO NACIONAL  
CHUQUISACA  
ASAMBLEA LEGISLATIVA PLURINACIONAL





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS



PROYECTO DE LEY  
LA ASAMBLEA LEGISLATIVA PLURINACIONAL

DECRETA:

PL-344/25

LEY INTEGRAL CONTRA LA VIOLENCIA DIGITAL

TÍTULO I: DISPOSICIONES GENERALES

**Artículo 1. (Objeto).** La presente Ley tiene por objeto prevenir, atender, sancionar y reparar la violencia digital, garantizando la protección de los derechos fundamentales en entornos digitales, conforme a los principios de legalidad y respeto a la libertad de expresión.

**Artículo 2. (Finalidad).** La presente Ley tiene como finalidad:

1. Garantizar a todas las personas el derecho a una vida libre de violencia en los entornos digitales.
2. Establecer mecanismos de prevención, protección y reparación frente a la violencia digital.
3. Fortalecer la institucionalidad del Estado para investigar y sancionar estas conductas.
4. Promover el uso seguro, responsable y respetuoso de las tecnologías digitales.
5. Regular la cooperación con intermediarios de internet en la prevención y respuesta a la violencia digital.

**Artículo 3 (Ámbito de aplicación).**

I. La presente Ley será aplicable a todas las personas naturales o jurídicas, e instituciones públicas o privadas, cuyas acciones u omisiones produzcan efectos en entornos digitales dentro del territorio del Estado Plurinacional de Bolivia.

II. Asimismo, será aplicable a los servicios digitales, intermediarios de internet y empresas de comunicación que ofrezcan servicios, tengan operaciones o dirijan sus actividades a personas usuarias situadas en el territorio del Estado Plurinacional de Bolivia, con independencia del lugar de su establecimiento, domicilio o de la ubicación de los servidores, plataformas o infraestructuras tecnológicas utilizadas.

III. La aplicación extraterritorial de la presente Ley se realizará conforme a los principios de legalidad, razonabilidad y jurisdicción efectiva, garantizando el respeto al derecho internacional y a los derechos fundamentales.

**Artículo 4. (Interpretación conforme a derechos humanos).**

La presente Ley se interpretará conforme a la Constitución Política del Estado y a los tratados internacionales de derechos humanos ratificados por el Estado, garantizando especialmente la libertad de expresión, la privacidad y el debido proceso.

**Artículo 5. (Garantía de libertad de expresión).**

I. Ninguna disposición de la presente Ley podrá ser interpretada o aplicada para restringir el ejercicio legítimo del derecho a la libertad de expresión y de información, incluyendo el periodismo, la crítica política, la sátira, la parodia, la





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

creación artística y la difusión de información de interés público, siempre que no afecte derechos de fundamentales.

II. Se encuentran especialmente protegidas las expresiones relacionadas con asuntos de interés público, el control social, la rendición de cuentas y el debate democrático.

III. Las medidas previstas en la presente Ley no constituyen mecanismos de censura previa. Cualquier responsabilidad derivada del ejercicio de la libertad de expresión será exclusivamente ulterior y deberá estar establecida por ley.

IV. Toda limitación al ejercicio de la libertad de expresión en el marco de la presente Ley deberá cumplir de manera estricta con los siguientes requisitos:

1. Estar prevista en una ley clara y precisa.
2. Perseguir una finalidad legítima, conforme a la Constitución y la legislación vigente.

V. En ningún caso la presente Ley podrá aplicarse para restringir expresiones que, aun cuando resulten críticas, incómodas o controversiales, se encuentren protegidas por el derecho a la libertad de expresión.

**Artículo 6. (Principios y garantías de aplicación).**

La interpretación y aplicación de la presente Ley se regirá por los siguientes principios legales:

1. Legalidad y seguridad jurídica.
2. Debido proceso.
3. Prohibición de censura previa.
4. Enfoque de derechos humanos, igualdad de género e interseccionalidad.

**Artículo 7. (Debida diligencia del Estado).**

I. El Estado, a través de las entidades competentes, deberá prevenir, investigar, sancionar y reparar la violencia digital, actuando con debida diligencia, de manera oportuna, efectiva y coordinada.

II. Esta obligación se ejercerá con debida diligencia reforzada en casos que involucren poblaciones en situación de vulnerabilidad, considerando sus condiciones específicas y riesgos diferenciados.

III. Las actuaciones estatales deberán garantizar el acceso a la justicia, la protección efectiva de las víctimas, la no revictimización y el respeto a los derechos fundamentales, en particular la libertad de expresión, la privacidad y el debido proceso.

IV. El Estado adoptará medidas de política pública, prevención, formación institucional y fortalecimiento de capacidades para asegurar el cumplimiento efectivo de las obligaciones previstas en la presente Ley.

**Artículo 8. (Definiciones).** Para efectos de esta Ley, se adoptan las siguientes definiciones:

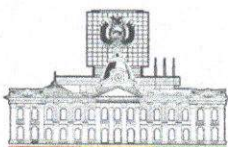
- a) **Violencia digital.** La violencia digital es cualquier acción, conducta u omisión, realizada mediante el uso de tecnologías de la información y la comunicación, que tenga por objeto o resultado causar daño, sufrimiento o afectar la dignidad, la integridad, la libertad, la vida privada o la seguridad de las personas.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

- b) Consentimiento digital:** El consentimiento para la captura o recepción de contenido íntimo no implica bajo ninguna circunstancia el consentimiento para su difusión o publicación.  
El consentimiento es específico, libre y revocable.  
La revocatoria del consentimiento obliga a quien posee el material a su eliminación inmediata. En caso de que el material ya haya sido difundido, la revocatoria faculta a la víctima a solicitar las medidas de protección previstas en la presente Ley.
- c) Entornos digitales.** Se entiende por entornos digitales los espacios de interacción, comunicación, creación, almacenamiento e intercambio de información que se desarrollan mediante tecnologías de información y comunicación, incluyendo internet, redes sociales, plataformas digitales, aplicaciones, servicios de mensajería y cualquier otro medio digital donde se generen, procesen o compartan contenidos e información.
- d) Datos personales.** Se entiende por datos personales toda información que identifique o haga identificable a una persona natural, de manera directa o indirecta, incluyendo datos de identidad, contacto, ubicación, imagen, voz, identificadores digitales u otra información que permita reconocerla o asociarla con su identidad.
- e) Contenido íntimo sexual.** Se entiende por contenido íntimo sexual a toda representación, descripción, imagen, audio, video o comunicación, en formato digital o impreso, de carácter real, manipulado o simulado, que involucre conductas sexuales explícitas, desnudez total o parcial, o la exhibición de partes íntimas del cuerpo humano con una connotación sexual o erótica. Este contenido pertenece estrictamente a la esfera privada y a la sexualidad de una persona, involucrando aspectos de su autonomía, consentimiento y dignidad que carecen de interés público.
- f) Contenido sexual simulado.** Se entiende por contenido sexual simulado todo material audiovisual, imagen, audio o representación digital que muestre o haga parecer que una persona participa en actos de carácter sexual o en la exposición de partes íntimas, sin que dicha situación haya ocurrido en la realidad, incluyendo contenidos creados, alterados o manipulados mediante tecnologías digitales.
- g) Difusión de contenidos falsos:** Información que se difunde masivamente de manera deliberada e intencionadamente, a sabiendas que es falsa. Solo será sancionable cuando constituya delito conforme a normativa vigente (fraude, extorsión u otros), no por su falsedad en sí misma.
- h) Desindexación digital:** Es la medida de protección y reparación mediante la cual se ordena a los proveedores de servicios de búsqueda en internet (motores de búsqueda), la desvinculación o ruptura del nexo técnico entre una consulta realizada a partir del nombre de una persona (u otros datos identificativos) y los resultados que dirigen a contenidos que constituyan violencia digital, vulneren la intimidad sexual o revictimicen a la persona afectada.  
Esta acción no implica la eliminación del contenido de la fuente original, sino la supresión de su visibilidad en las listas de resultados de búsqueda, con el fin de garantizar el derecho al honor, la propia imagen y la vida privada. La desindexación deberá ser proporcional y no se aplicará a información de interés público, procesos penales por corrupción o crímenes de lesa humanidad, para evitar el borrado de memoria histórica.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

- i) **Intermediarios de internet:** Se entenderá por intermediarios de internet a toda persona natural o jurídica que, en calidad de proveedor de servicios digitales, facilite, posibilite o medie el acceso, transmisión, almacenamiento, alojamiento, indexación, difusión o puesta a disposición de contenidos, datos o comunicaciones generadas por terceros a través de redes digitales. Estos incluyen, de manera enunciativa y no limitativa, a proveedores de acceso a internet, servicios de alojamiento, redes sociales, motores de búsqueda, servicios de mensajería, plataformas de intercambio de contenidos y otros servicios equivalentes.
- j) **Empresas de comunicación:** Se entenderá por empresas de comunicación a toda persona natural o jurídica, pública o privada, que de manera autorizada presta servicios de transmisión, acceso, conexión o gestión de comunicaciones y datos a través de redes de telecomunicaciones o medios digitales.
- Estas empresas comprenden, entre otras, a los proveedores de acceso a internet, operadores de redes, servicios móviles, servicios de datos y otros servicios equivalentes vinculados a las tecnologías de la información y comunicación.
- k) **Plataformas digitales:** Las plataformas digitales implican todo entorno o espacio accesible mediante internet u otros medios electrónicos, diseñado para la interacción, difusión, almacenamiento, transmisión o generación de contenido digital entre personas u organizaciones. Las plataformas digitales comprenden, entre otras:
1. Redes sociales.
  2. Plataformas de mensajería.
  3. Aplicaciones de video llamadas o chats en línea.
  4. Servicios de alojamiento de contenidos.
  5. Foros, blogs, páginas web y juegos en línea con interacción social.

**n) Contenido ilícito**

Se entenderá por contenido ilícito todo aquel que, por su naturaleza o por las circunstancias en las que se produce, difunde o pone a disposición, constituye una infracción al ordenamiento jurídico vigente y ha sido calificado como tal por autoridad competente.

**o) Contenidos dañinos**

Se entenderá por contenidos dañinos aquellos que, sin constituir ilícito penal, pueden generar afectaciones a derechos fundamentales en contextos de violencia digital.

Su identificación tendrá fines exclusivamente preventivos, educativos o de política pública, y en ningún caso dará lugar a sanciones ni restricciones al ejercicio de la libertad de expresión fuera de los supuestos previstos expresamente por la ley.

**Artículo 9. (Derechos en entornos digitales).**

I. Toda persona tiene derecho a ejercer plenamente sus derechos y libertades fundamentales en los entornos digitales, en condiciones de igualdad, dignidad y no discriminación.

II. En el marco de la presente Ley, el Estado garantiza los siguientes derechos en los entornos digitales:

1. **Derecho a una vida libre de violencia digital**, que comprende la protección frente a cualquier forma de agresión, hostigamiento, intimidación,





## ASAMBLEA LEGISLATIVA PLURINACIONAL CÁMARA DE DIPUTADOS

explotación o abuso cometido mediante tecnologías de la información y comunicación. Asimismo, toda persona tiene derecho a participar en entornos digitales libres de violencia, discriminación y acoso.

2. **Derecho a la privacidad y a la protección de datos personales**, incluyendo el control sobre la recopilación, tratamiento, almacenamiento y difusión de información personal.
3. **Derecho a la libertad de expresión y al acceso a la información**, conforme a la Constitución Política del Estado y a los tratados internacionales de derechos humanos.
4. **Derecho a la seguridad y autonomía digital**, que comprende la protección frente al acceso no autorizado a cuentas, dispositivos o sistemas, así como frente a prácticas tecnológicas que vulneren la integridad y dignidad de las personas.
5. **Derecho al consentimiento** en el uso, producción y difusión de imágenes, datos y contenidos personales en entornos digitales.
6. **Derecho al acceso a mecanismos efectivos de denuncia**, protección, atención y reparación frente a hechos de violencia digital.
7. **Derecho a la desindexación**, a solicitar la eliminación o desvinculación de los motores de búsqueda de contenidos que constituyan violencia digital, especialmente cuando medie una resolución judicial o administrativa que reconozca la agresión.
8. **Derecho a la seguridad desde el diseño**, a que los servicios y plataformas digitales incorporen salvaguardas técnicas por defecto que prevengan el uso malicioso de la tecnología y protejan la integridad de los usuarios.
9. **Derecho a la alfabetización digital**, a recibir educación formal y no formal sobre el uso ético, seguro y responsable de las tecnologías, con un enfoque que permita identificar riesgos y desmontar estereotipos de género.

III. El Estado adoptará medidas legislativas, institucionales, educativas y tecnológicas necesarias para garantizar el ejercicio efectivo de estos derechos, promoviendo entornos digitales seguros, libres de violencia y respetuosos de los derechos humanos.

## TÍTULO II: PREVENCIÓN DE LA VIOLENCIA DIGITAL

### CAPÍTULO I: POLÍTICAS PÚBLICAS PREVENTIVAS ANTE LA VIOLENCIA DIGITAL

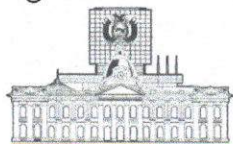
#### Artículo 10. (Autoridad rectora).

El Ministerio de la Presidencia, a través de la entidad competente en materia de tecnologías de la información y comunicación, será responsable de la coordinación, implementación y seguimiento de la presente Ley.

#### Artículo 11. (Políticas públicas de prevención).

El Órgano Ejecutivo a través de los ministerios competentes, en coordinación con las entidades territoriales autónomas, desarrollará políticas públicas para:

1. Prevenir la violencia digital mediante acciones educativas, informativas y comunitarias.
2. Promover una cultura de respeto, consentimiento y responsabilidad en los entornos digitales.
3. Reducir los riesgos asociados al uso de tecnologías digitales.
4. Fortalecer las capacidades institucionales para la prevención y detección temprana de la violencia digital.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**CAPÍTULO II: MEDIDAS EN EL ÁMBITO EDUCATIVO**

**Artículo 12. (Educación y alfabetización digital en el sistema educativo).**

- I. El Ministerio de Educación incorporará de manera progresiva en los planes y programas de estudio de todos los niveles y modalidades del sistema educativo contenidos orientados a fortalecer la educación y alfabetización digital.
- II. Estas acciones educativas priorizarán a poblaciones en situación de vulnerabilidad y estarán orientadas al fortalecimiento de capacidades para el uso seguro, ético y responsable de las tecnologías digitales, así como a la prevención de la violencia digital y el desarrollo de prácticas de cuidado digital.

**Artículo 13. (Política pública de educación, alfabetización digital y prevención de la violencia digital).**

- I. El Ministerio de Educación, a través de las entidades competentes, diseñará e implementará políticas públicas integrales de educación, alfabetización digital y prevención de la violencia digital, con alcance nacional e intersectorial.
- II. Estas políticas públicas se regirán por los principios de derechos humanos, igualdad de género e interseccionalidad, con especial atención a mujeres, niñas, niños, adolescentes y poblaciones en situación de vulnerabilidad.
- III. El diseño, implementación y evaluación de estas políticas deberá realizarse con la participación de la sociedad civil, la academia, el sector privado y otros actores relevantes.

**CAPÍTULO III: MEDIDAS EN EL ÁMBITO COMUNICACIONAL**

**Artículo 14. (Política comunicacional para la prevención de la violencia digital).**

- I. El Ministerio de la Presidencia, en coordinación con los ministerios competentes y con la participación de instituciones públicas y privadas, elaborará e implementará una política comunicacional orientada a la prevención de la violencia digital, incorporando enfoques de derechos humanos, género, interculturalidad y generacional, considerando la diversidad de la población y sus distintas necesidades.
- II. Esta política deberá contemplar, entre otros, los siguientes objetivos:
  1. Visibilizar y sensibilizar a la población sobre las distintas formas de violencia digital.
  2. Informar y promover el conocimiento de los derechos en los entornos digitales.
  3. Fomentar el uso seguro, responsable y respetuoso de las tecnologías de la información y comunicación.
  4. Difundir de manera accesible los mecanismos de denuncia, atención y protección frente a hechos de violencia digital.
  5. Las campañas comunicacionales deberán prestar especial atención a niñas, niños, adolescentes, mujeres y otros grupos en situación de vulnerabilidad.

**CAPÍTULO IV: FORMACIÓN ESPECIALIZADA A SERVIDORES PÚBLICOS**

**Artículo 15. (Formación especializada a servidoras y servidores públicos).**

- I. Las instituciones del Estado con competencias en la prevención, atención, investigación y sanción de la violencia digital deberán implementar programas



## ASAMBLEA LEGISLATIVA PLURINACIONAL CÁMARA DE DIPUTADOS

permanentes de formación y capacitación especializada dirigidas a servidoras y servidores públicos, con el fin de fortalecer sus capacidades para prevenir, identificar, investigar y atender casos de violencia digital.

II. Estos programas deberán ser desarrollados, entre otros, en:

1. La Escuela de Jueces del Estado.
2. La Escuela de Fiscales del Estado.
3. Las entidades de formación, especialización y capacitación de la Policía Boliviana.
4. Las instituciones de formación superior vinculadas a la administración de justicia y seguridad pública.
5. El sistema educativo en todos sus niveles, mediante la capacitación de educadoras y educadores.
6. La Escuela de Gestión Pública Plurinacional brindará formación especializada a los y las servidoras públicas con competencias en material de violencia digital

III. Los procesos de formación deberán incorporar enfoques de derechos humanos, género, interseccionalidad y protección de víctimas, garantizando una atención adecuada, oportuna y libre de revictimización.

### **CAPÍTULO V: GENERACIÓN DE DATOS, ESTADÍSTICAS, INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍAS DIGITALES**

#### **Artículo 16. (Generación de datos estadísticos e investigación).**

I. El Ministerio de Gobierno, en coordinación con los ministerios e instituciones públicas competentes crearán el Observatorio Nacional de Violencia Digital, con el fin de monitorear tendencias, riesgos y políticas públicas, generar y sistematizar datos estadísticos sobre la situación de la violencia digital en el Estado Plurinacional de Bolivia.

II. El Observatorio Nacional de Violencia Digital promoverá la investigación, producción de conocimiento y generación de información sobre violencia digital, con el fin de fortalecer el diseño, implementación y evaluación de políticas públicas basadas en evidencia.

III. La generación, tratamiento y difusión de datos estadísticos e investigaciones deberá realizarse respetando los estándares éticos, la protección de datos personales, los principios de datos abiertos cuando corresponda, garantizando la protección del derecho a la intimidad, dignidad y seguridad de las víctimas y de su entorno.

#### **Artículo 17. (Registro de información para fines de investigación y prevención).**

I. El Ministerio de Gobierno, a través del Observatorio Nacional de Violencia Digital, podrá gestionar sistemas de información orientados a la prevención, análisis y seguimiento de la violencia digital, con fines exclusivamente estadísticos, de política pública e investigación.

II. La incorporación de información identificable en estos sistemas únicamente procederá cuando exista una investigación formal iniciada por autoridad competente, o medie orden judicial debidamente fundamentada.

III. En ningún caso estos sistemas podrán constituir registros públicos de personas denunciadas; generar estigmatización o presunción de culpabilidad; ser utilizados con fines distintos a los establecidos en la presente Ley.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**IV.** Como parte de la base de datos se creará y administrará una Base Nacional de Números Telefónicos Vinculados a Casos de Violencia Digital, el registro de números se basará en los procesos judiciales o procesos de investigación en abiertos.

**V.** Se garantizará el derecho de acceso, rectificación, actualización y supresión de los datos, conforme al debido proceso.

**VI.** La información deberá ser tratada bajo estrictos estándares de confidencialidad, seguridad y proporcionalidad, evitando la identificación de víctimas y personas no condenadas.

**VII.** El Ministerio de Gobierno deberá establecer protocolos claros para el acceso, actualización y uso de la Base, garantizando la transparencia y trazabilidad de las acciones, y produciendo informes periódicos con insumos estadísticos y de política pública, respetando siempre la anonimización de datos sensibles de las víctimas y respetando los derechos de las personas agresoras.

**VIII.** El Ministerio de Gobierno usará los datos de la Base de Datos para coadyuvar con los procesos judiciales.

**Artículo 18. (Códigos de ética en el desarrollo de tecnologías digitales).**

**I.** El Ministerio de la Presidencia promoverá el desarrollo, implementación y adopción de códigos de ética y estándares de responsabilidad en el diseño, desarrollo, implementación y uso de tecnologías digitales, con el fin de prevenir la violencia digital y garantizar el respeto de los derechos humanos en los entornos digitales.

**II.** Las entidades públicas, instituciones académicas, centros de investigación, empresas tecnológicas y otros actores involucrados en el desarrollo o implementación de tecnologías digitales deberán incorporar principios éticos orientados a:

1. Prevenir la generación, reproducción o amplificación de prácticas de violencia digital, discriminación o abuso mediante tecnologías digitales.
2. Garantizar que el diseño y funcionamiento de tecnologías digitales considere la protección de la dignidad, privacidad, seguridad y derechos de las personas usuarias.
3. Promover el desarrollo de tecnologías seguras y responsables que incorporen medidas de prevención frente al acoso digital, la difusión no consentida de contenido íntimo y otras formas de violencia digital.
4. Identificar, prevenir y mitigar riesgos asociados al uso de sistemas automatizados, algoritmos y otras tecnologías emergentes que puedan generar daños a las personas.
5. Fomentar la transparencia, la rendición de cuentas y la responsabilidad en el desarrollo y uso de tecnologías digitales.

**III.** El Estado promoverá espacios de coordinación con el sector tecnológico, la academia y la sociedad civil para impulsar buenas prácticas y estándares éticos en el desarrollo de tecnologías digitales, priorizando la protección de los derechos humanos y la prevención de la violencia digital.

**Artículo 19. (Protección de datos personales).**

**I.** El tratamiento de datos personales en el marco de la presente Ley deberá realizarse conforme a los principios de legalidad, finalidad, seguridad y confidencialidad, garantizando en todo momento el respeto a la dignidad, privacidad y derechos de las personas.

**II.** El tratamiento de datos deberá limitarse estrictamente a lo necesario para el cumplimiento de los fines previstos en la presente Ley, quedando prohibida





## ASAMBLEA LEGISLATIVA PLURINACIONAL CÁMARA DE DIPUTADOS

cualquier forma de recopilación, almacenamiento, uso o conservación excesiva, arbitraria o no justificada, respetando el debido proceso.

**III.** El acceso, conservación o entrega de datos personales, datos de tráfico o información vinculada a comunicaciones sólo procederá mediante orden de autoridad competente, debidamente fundamentada.

**IV.** Las autoridades y sujetos obligados deberán adoptar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, prevenir accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.

**V.** En ningún caso el tratamiento de datos personales podrá utilizarse para fines distintos a los previstos en la presente Ley ni dar lugar a prácticas de vigilancia masiva o desproporcionada.

### **Artículo 20. (Tratamiento de datos y deberes de colaboración de las empresas de comunicación e intermediarios de internet).**

**I.** Las empresas de comunicación y los intermediarios de internet únicamente estarán obligados a conservar, acceder o proporcionar datos personales cuando medie orden emitida por autoridad judicial competente, debidamente fundamentada, específica y proporcional, conforme a la Constitución y la normativa vigente.

**II.** Se prohíbe la retención masiva, indiscriminada o preventiva de datos personales, así como cualquier forma de tratamiento que no se ajuste a los principios de legalidad.

**III.** Las obligaciones previstas en el presente artículo no podrán interpretarse ni aplicarse en el sentido de imponer deberes generales de monitoreo, vigilancia o supervisión previa de contenidos.

**IV.** Toda actuación en el marco del presente artículo deberá respetar el debido proceso, la confidencialidad de las comunicaciones y las garantías de protección de datos personales.

## **CAPÍTULO VI: ALERTAS DIGITALES**

### **Artículo 21. (Alertas digitales).**

**I.** El Ministerio de Gobierno a través del Observatorio Nacional de Violencia Digital en coordinación con las entidades competentes, implementará mecanismos de alertas digitales con el propósito de informar y prevenir a la población sobre riesgos, modalidades y patrones de comisión de violencia digital, así como sobre prácticas que puedan afectar la seguridad, privacidad y derechos de las personas en los entornos digitales.

**II.** Las alertas digitales consistirán en la difusión oportuna de información preventiva, reportes públicos y comunicaciones dirigidas a la población, orientadas a:

- 1.** Informar sobre nuevas modalidades o formas de violencia digital y los modos de operación utilizados por personas agresoras.
- 2.** Informar sobre el uso de sistemas automatizados.
- 3.** Advertir sobre riesgos emergentes vinculados al uso de tecnologías digitales que puedan afectar la seguridad o integridad de las personas.
- 4.** Promover medidas de prevención, autocuidado y seguridad digital.
- 5.** Difundir mecanismos de denuncia, orientación y atención disponibles para las víctimas.

**III.** Las alertas digitales deberán difundirse mediante campañas informativas, plataformas digitales, medios de comunicación y otros canales accesibles para la





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

población, garantizando un enfoque preventivo, educativo y de protección de derechos.

**IV.** La emisión de alertas digitales deberá respetar los principios de veracidad, protección de datos personales y confidencialidad, evitando la exposición o revictimización de personas afectadas.

**CAPÍTULO VII: CORRESPONSABILIDAD EN LA GENERACIÓN DE CONTENIDO DIGITAL**

**Artículo 22. (Corresponsabilidad de medios digitales y generadores de contenido).**

**I.** El Estado promoverá mecanismos de corresponsabilidad, autorregulación y buenas prácticas orientados a prevenir la violencia digital en la producción, publicación y difusión de contenidos digitales.

A tal efecto, se promoverá:

1. La adopción de códigos de ética y lineamientos editoriales que incorporen criterios de respeto a los derechos humanos y prevención de la violencia digital.
2. La implementación de mecanismos internos de reporte, revisión y retiro de contenidos que constituyan violencia digital, conforme a la normativa vigente y respetando el debido proceso.
3. La promoción de contenidos responsables y libres de violencia, que contribuyan a la construcción de entornos digitales seguros, respetuosos e inclusivos.
4. El desarrollo de programas de formación y sensibilización dirigidos a periodistas, comunicadores y personas generadoras de contenido digital sobre derechos humanos, violencia digital y ética en la comunicación digital.

**II.** Los medios de comunicación digitales, plataformas de difusión de contenidos y personas generadoras de contenido digital tienen el deber de ejercer su actividad con responsabilidad social, respetando los derechos fundamentales de las personas en los entornos digitales.

**III.** Las medidas promovidas en el marco del presente artículo deberán garantizar el respeto al derecho a la libertad de expresión, el pluralismo informativo y el acceso a la información, conforme a la Constitución Política del Estado y a los tratados internacionales de derechos humanos ratificados por el Estado.

**Artículo 23. (Acuerdos de cooperación y correulación con intermediarios de internet).**

**I.** El Estado, a través de las entidades competentes, promoverá mecanismos de cooperación y correulación a través de la suscripción acuerdos conjuntos con los intermediarios de internet que presten servicios a personas usuarias situadas en el territorio del Estado Plurinacional de Bolivia, con el propósito de prevenir, mitigar, investigar y atender la violencia digital, incluyendo sus manifestaciones individuales y sistémicas, garantizando el respeto a los derechos fundamentales.

**II.** En el marco de estos acuerdos, el Estado establecerá principios y estándares generales, mientras que los intermediarios de internet adoptarán políticas, mecanismos y procedimientos propios para su implementación, conforme a la presente Ley.

**III.** Los acuerdos de cooperación y correulación deberán incorporar un enfoque de gestión de riesgos, que incluya la identificación, análisis y mitigación de riesgos sistémicos asociados a la violencia digital, entendidos como aquellos derivados de:





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

1. La difusión masiva o amplificación algorítmica de contenidos que constituyan violencia digital.
  2. La existencia de campañas coordinadas de acoso, hostigamiento o desinformación dirigidas contra personas o grupos en situación de vulnerabilidad.
  3. El uso abusivo o malicioso de funcionalidades de las plataformas que faciliten la revictimización o el daño reiterado.
- IV. La implementación y evaluación de estos acuerdos deberá garantizar:
1. Transparencia en su aplicación.
  2. Acceso a información relevante por parte de las autoridades competentes.
  3. Participación de la sociedad civil, la academia y actores especializados en derechos digitales y derechos fundamentales.

**Artículo 24. (Responsabilidad de los intermediarios de internet)**

- I. Los intermediarios de internet no serán responsables por los contenidos generados, alojados o transmitidos por terceros, en el marco de la prestación de sus servicios.
- II. Excepcionalmente, podrán ser considerados responsables cuando:
1. Medie orden emitida por autoridad competente, conforme a la normativa vigente y en observancia de los principios de legalidad.
  2. No hayan adoptado, de manera injustificada, medidas razonables y oportunas para su cumplimiento.
- III. Las medidas adoptadas en aplicación de este artículo deberán respetar el debido proceso, garantizando, prioritariamente:
1. La notificación a la persona identificada, cuando corresponda.
  2. El derecho a la defensa.
  3. El acceso a mecanismos efectivos de impugnación.
- IV. Las disposiciones del presente artículo no podrán interpretarse en el sentido de imponer obligaciones generales de monitoreo, vigilancia o supervisión previa de contenidos.

**TÍTULO III: MEDIDAS DE PROTECCIÓN,  
ATENCIÓN Y REPARACIÓN DE LAS VÍCTIMAS**

**CAPÍTULO I: MEDIDAS DE PROTECCIÓN A VÍCTIMAS DE VIOLENCIA DIGITAL**

**Artículo 25. (Tipos de medidas de protección digital).**

- I. En concordancia con la normativa vigente, las medidas de protección digital tienen por finalidad prevenir, detener y reparar situaciones de violencia digital, garantizando la protección efectiva de los derechos de la víctima.
- II. Las autoridades competentes deberán disponer, de manera individual o conjunta, entre otras, las siguientes medidas:
1. Desindexación de contenidos en motores de búsqueda.
  2. Eliminación, bloqueo o limitación de acceso a contenidos digitales.
  3. Suspensión, bloqueo o inhabilitación de cuentas, perfiles o servicios digitales utilizados para la agresión.
  4. Protección de la identidad de la víctima, incluyendo la anonimización de datos personales.
  5. Prohibición de contacto, interacción o acercamiento a través de medios digitales.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

6. Etiquetado, advertencias u otras medidas informativas sobre contenidos, cuando corresponda.
7. Preservación de evidencia digital.
8. Otras medidas necesarias, idóneas y proporcionales para la protección de los derechos.

III. Las medidas deberán respetar los derechos fundamentales.

**Artículo 26. (Medidas de protección urgentes en casos de violencia digital).**

I. En casos de violencia digital, el Ministerio Público o la autoridad judicial competente, de oficio o a petición de parte, ordenará en un plazo máximo de veinticuatro (24) horas las siguientes medidas:

1. Interrupción o bloqueo preventivo de la difusión de los contenidos denunciados.
2. Orden de desindexación a los motores de búsqueda para evitar que el contenido sea hallado mediante nombres o palabras clave.
3. Preservación de evidencia digital, ordenando a los proveedores de servicios el resguardo de registros de acceso (logs), direcciones IP y metadatos por un tiempo no menor a noventa (90) días.
4. Apoyo psicológico en los casos donde se requiera.

II. El incumplimiento de estas medidas por parte de intermediarios locales dará lugar a sanciones administrativas y multas progresivas, sin perjuicio de la responsabilidad penal por desobediencia a resoluciones judiciales.

**Artículo 27. (Procedimiento para medidas de protección digital).**

I. Las solicitudes de medidas de protección digital se tramitarán mediante un procedimiento breve, expedito y gratuito, orientado a la tutela efectiva de derechos.

II. El o la juez competente deberá resolver en un plazo máximo de setenta y dos (72) horas. En casos de urgencia, podrá disponer medidas cautelares en un plazo no mayor a cuarenta y ocho (48) horas.

III. Las medidas podrán adoptarse cuando exista una probabilidad razonable de afectación a derechos y riesgo de:

1. Daño.
2. Revictimización.
3. Difusión persistente o reiterada del contenido.
4. Afectación a los derechos reconocidos en la presente ley.

IV. La valoración se realizará conforme a criterios de razonabilidad y proporcionalidad.

V. El procedimiento deberá garantizar:

1. No revictimización.
2. Confidencialidad.
3. Protección de datos personales.
4. Accesibilidad y adecuación a la persona solicitante.

VI. Las decisiones deberán ser fundamentadas y susceptibles de impugnación conforme a la normativa vigente.

VII. En caso de plataformas digitales domiciliadas fuera del territorio nacional, el Ministerio Público, a través de la cooperación internacional solicitará la preservación y remoción de datos.

VIII. Se establece la obligación para proveedores locales de servicios de internet (ISPs) de cumplir con el bloqueo de acceso a sitios de explotación sexual digital en un plazo máximo de 24 horas bajo orden judicial.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**Artículo 28. (Principios para la restricción de contenidos digitales).**

Toda medida que implique la restricción, eliminación, bloqueo o desindexación de contenidos digitales deberá:

1. Estar prevista en la ley.
2. Perseguir una finalidad legítima, como la protección de derechos fundamentales.
3. Ser necesaria e idónea para evitar un daño.
4. Ser proporcional en sentido estricto.

Estas medidas deberán ser dispuestas por autoridad competente, y serán aplicadas caso por caso, garantizando el debido proceso.

**Artículo 29. (Confidencialidad y protección de la identidad de la víctima).**

I. En los procesos judiciales o administrativos relacionados con hechos de violencia digital, las autoridades competentes deberán garantizar la confidencialidad y el resguardo de la identidad, imagen, datos personales e información sensible de la víctima durante todas las etapas del proceso.

II. Queda prohibida la difusión, publicación o reproducción de información que permita identificar directa o indirectamente a la víctima, a través de medios de comunicación, plataformas digitales, redes sociales u otros medios de difusión pública, salvo autorización expresa de la persona afectada o cuando dicha información sea necesaria para la investigación o el proceso judicial, conforme a la normativa vigente.

III. Las autoridades deberán adoptar las medidas necesarias para evitar la exposición pública, la revictimización y cualquier forma de afectación a la dignidad, privacidad e integridad de la víctima, garantizando el respeto de sus derechos y la protección de su seguridad personal y digital.

**Artículo 30. (Prohibición de monitoreo general y censura indirecta).**

Ninguna disposición de la presente Ley podrá interpretarse en el sentido de imponer a los intermediarios de internet obligaciones generales de monitoreo, supervisión o filtrado previo de contenidos, ni de habilitar mecanismos de censura directa o indirecta.

**CAPÍTULO II: MEDIDAS DE REPARACIÓN A VÍCTIMAS DE VIOLENCIA DIGITAL**

**Artículo 31. (Derecho a la reparación integral)**

I. Toda persona víctima de violencia digital tiene derecho a una reparación integral, oportuna y efectiva, orientada a restituir los derechos vulnerados y garantizar su dignidad, integridad física, psicológica, sexual y emocional, así como su seguridad en entornos digitales.

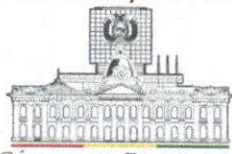
II. Las autoridades competentes deberán garantizar la protección de la víctima durante todas las etapas del proceso, evitando su revictimización y pudiendo disponer medidas de reparación integral, incluyendo asistencia psicológica, social o terapéutica especializada.

III. En ningún caso se dispondrán medidas de imposible cumplimiento.

**Artículo 32. (Contenido de la reparación integral).**

I. La reparación integral comprenderá, según corresponda, medidas de:

1. **Restitución:** incluyendo la eliminación, desindexación o limitación de acceso a contenidos digitales que constituyan violencia digital.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

2. **Rehabilitación:** mediante atención psicológica, social o terapéutica especializada.
  3. **Satisfacción:** tales como la rectificación, aclaración pública u otras medidas orientadas al restablecimiento de la dignidad de la víctima.
  4. **Indemnización:** de acuerdo a la valoración de la afectación y valoración judicial según normativa vigente.
  5. **Garantías de no repetición:** incluyendo medidas orientadas a prevenir la reiteración de los hechos y proteger los datos personales de la víctima.
- II. Las medidas de reparación integral descritas en el párrafo anterior serán determinadas por la autoridad judicial competente que conoció la causa.

**Artículo 33. (Medidas de desindexación y eliminación de difusión de contenidos).**

- I. Como parte de la reparación integral, las víctimas podrán solicitar la desindexación y eliminación de la difusión de contenidos digitales que constituyan violencia digital, previa determinación mediante resolución de autoridad competente.
- II. Las autoridades podrán disponer las medidas necesarias para eliminar, bloquear o limitar el acceso al contenido, cuando ello sea técnica y jurídicamente posible, garantizando la protección de la dignidad, privacidad e integridad de la víctima, en equilibrio con la libertad de expresión y el acceso a la información.
- III. Estas medidas no constituyen censura previa y deberán aplicarse de manera excepcional, caso por caso, conforme al principio de legalidad.
- IV. La desindexación o eliminación de contenido violento procederá para garantizar el ejercicio de derechos de las personas en entornos digitales.

**Artículo 34. (Reparación integral y eliminación de huella digital).**

- I. La reparación integral de las víctimas de violencia digital deberá incluir medidas especializadas para la eliminación o mitigación de la huella digital de los contenidos con violencia digital en motores de búsqueda y plataformas digitales.
- II. Las medidas comprenderán:
  - a. Solicitudes de retiro o bloqueo de contenidos, enlaces y resultados de búsqueda asociados al contenido con violencia digital.
  - b. Emisión de alertas de rectificación en los mismos espacios donde se produjo la agresión, cuando ello sea pertinente y técnicamente viable.
  - c. Orientación a la víctima sobre herramientas y procedimientos para la protección de su identidad y privacidad en línea.
- III. Las autoridades competentes deberán coordinar con los intermediarios de internet y empresas de comunicación para asegurar la efectividad de la reparación, manteniendo registros de las acciones realizadas y sus resultados.

**CAPÍTULO III: COOPERACIÓN ENTRE ESTADOS Y COORDINACIÓN CON LA SOCIEDAD CIVIL**

**Artículo 35. (Cooperación entre Estados).**

- I. El Estado promoverá mecanismos de cooperación internacional para la prevención, investigación y sanción de la violencia digital, en el marco de la Constitución Política del Estado, los tratados internacionales ratificados y la normativa nacional aplicable.
- II. A tal efecto, las autoridades competentes podrán:





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

1. Establecer acuerdos bilaterales que permitan la cooperación entre autoridades para la investigación de hechos de violencia digital, incluyendo la conformación de mecanismos de investigación conjunta.
  2. Garantizar la asistencia mutua entre autoridades, mediante canales de comunicación rápidos y seguros para el intercambio de información relevante en investigaciones o procesos judiciales, en el marco de la normativa vigente.
  3. Colaborar en la obtención, preservación y transmisión de evidencia digital, conforme a los instrumentos internacionales y a las garantías del debido proceso.
  4. Facilitar el intercambio de información, experiencias y buenas prácticas en materia de legislación, políticas públicas y mecanismos de prevención y respuesta frente a la violencia digital.
- III. Las solicitudes de cooperación internacional podrán ser rechazadas cuando existan motivos fundados para considerar que tienen como finalidad la persecución o discriminación de una persona.

**Artículo 36. (Articulación con la sociedad civil).**

I. El Estado promoverá la articulación y colaboración con organizaciones de la sociedad civil, academia, sector tecnológico y otros actores sociales, con el propósito de fortalecer las acciones de:

1. Prevención,
2. Generación y gestión del conocimiento,
3. Identificación de casos y riesgos,
4. Derivación y/o acompañamiento de casos de violencia digital,
5. Acciones de vigilancia y control social.

II. Las acciones de articulación deberán promover la participación efectiva de las organizaciones especializadas en derechos humanos, derechos digitales, personas naturales o jurídicas que acompañan a víctimas, respetando los principios de transparencia, colaboración y enfoque de derechos humanos.

**TÍTULO IV: PROCESO JUDICIAL**

**CAPÍTULO I: PROCEDIMIENTO PENAL PARA DELITOS DE VIOLENCIA DIGITAL**

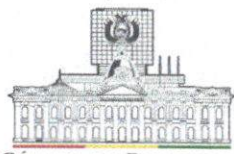
**Artículo 37. (Delitos de violencia digital).**

Los delitos de violencia digital son de acción pública, la denuncia podrá ser presentada por la víctima, por cualquier persona natural o jurídica que tenga conocimiento del hecho, o iniciarse de oficio por las autoridades competentes.

**Artículo 38. (Jurisdicción extraterritorial).**

I. Las autoridades jurisdiccionales del Estado Plurinacional de Bolivia serán competentes para conocer, investigar, juzgar y sancionar los hechos de violencia digital previstos en la presente Ley cuando sus efectos se produzcan en el territorio nacional o cuando la conducta afecte a personas que se encuentren en él, aun cuando la acción haya sido realizada total o parcialmente desde el extranjero, o mediante infraestructuras tecnológicas, plataformas digitales o servidores ubicados fuera del país.

II. En estos casos, la investigación y persecución de los hechos se realizará conforme a la Constitución Política del Estado, la legislación nacional vigente y los instrumentos internacionales de cooperación y asistencia mutua en materia penal aplicables.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**Artículo 39. (Medios de prueba y principio de informalidad).**

I. En los procesos relacionados con hechos de violencia digital se admitirán como medios de prueba todos los elementos de convicción que permitan conocer los hechos denunciados, incluyendo registros, capturas de pantalla, enlaces, comunicaciones electrónicas, metadatos u otros medios digitales.

II. La presentación de la denuncia y de los elementos probatorios estará sujeto al principio de informalidad, debiendo las autoridades competentes aplicar medidas que faciliten el acceso a la justicia y eviten la revictimización.

**Artículo 40. (Carga de la prueba).**

En todo proceso penal por hechos de violencia digital, la carga de la prueba corresponderá al Ministerio Público y no así a la víctima.

**Artículo 41. (Validez de la evidencia digital).**

I. Las impresiones de mensajes, capturas de pantalla, archivos de audio, video y cualquier dato almacenado en dispositivos electrónicos o la "nube" tendrán valor probatorio de indicio.

II. Para alcanzar valor de prueba plena, la autoridad competente deberá garantizar la integridad mediante el cotejo con el dispositivo origen o la certificación de metadatos, siguiendo protocolos de cadena de custodia digital establecidos por el IDIF.

**Artículo 42. (Resguardo de evidencia digital y valoración).**

I. Las autoridades judiciales, fiscales y policiales deberán garantizar el resguardo, preservación y adecuada gestión de la evidencia digital, aplicando protocolos técnicos de recopilación, conservación y análisis que aseguren su integridad y autenticidad.

II. La valoración de la prueba corresponderá a la jueza o al juez, quien deberá fundamentar su decisión conforme a las reglas de la sana crítica y a los principios de protección de las víctimas.

**Artículo 43. (Validez y cadena de custodia digital).**

I. Las capturas de pantalla, grabaciones de audio y video, archivos de mensajería instantánea, correos electrónicos y metadatos de archivos multimedia tienen valor probatorio pleno siempre que se garantice su integridad.

II. El Instituto de Investigaciones Forenses (IDIF) establecerá un protocolo simplificado de cadena de custodia digital para que las víctimas puedan presentar evidencia inicial sin riesgo de exclusión probatoria.

III. La ausencia de peritos especializados en áreas rurales no será causa de rechazo de la denuncia; se deberá proceder a la preservación del dispositivo origen.

**Artículo 44. (Protocolos especializados de actuación).**

I. El Ministerio Público y el Órgano Judicial y las demás entidades públicas competentes deberán elaborar, actualizar e implementar protocolos especializados de actuación para la prevención, atención, investigación y sanción de hechos de violencia digital.

II. Estos protocolos deberán establecer procedimientos claros y coordinados para la recepción de denuncias, la recolección, resguardo y preservación de evidencia digital; creando la cadena de custodia de delitos de violencia digital.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

III. Incorporar la adopción inmediata de medidas de protección y la atención integral a las víctimas en los casos que corresponda.

IV. Asimismo, deberán garantizar el acceso efectivo a la justicia, la protección de la dignidad, privacidad e integridad de las víctimas, evitando su revictimización y asegurando procesos oportunos, diligentes y con enfoque de derechos humanos.

**CAPÍTULO II: RÉGIMEN APLICABLE PARA NIÑAS, NIÑOS Y ADOLESCENTES**

**Artículo 45. (Tratamiento de niñas, niños y adolescentes).**

Cuando los hechos de violencia digital previstos en la presente Ley sean cometidos por niñas, niños o adolescentes, su tratamiento se regirá por lo establecido en la Ley 548, de 17 de julio de 2014, Código Niña, Niño y Adolescente y la normativa especializada vigente.

**Artículo 46. (Medidas socioeducativas).**

I. En los casos previstos en el artículo anterior las instancias competentes a nivel nacional y subnacional en coordinación dispondrán medidas socioeducativas, o de orientación, conforme a la legislación especializada en materia de niñez y adolescencia, con el objetivo de promover la responsabilización del adolescente, la reparación del daño y la prevención de nuevas conductas de violencia digital.

II. Además de las medidas socioeducativas establecidas en la Ley 548, el 17 de julio de 2014, Código Niña, Niño y Adolescente, las autoridades competentes deberán formarse en la aplicación de medidas socioeducativas adaptadas a entornos digitales que contemple como mínimo:

- a. Prevención de la violencia digital y uso responsable de las tecnologías.
- b. Restricciones supervisadas en el uso de tecnologías digitales o plataformas relacionadas con los hechos.
- c. Medidas de orientación dirigidas a madres, padres, responsables legales, educadores, promoviendo su corresponsabilidad en la prevención de la violencia digital.

III. La aplicación de estas medidas deberá evitar toda forma de estigmatización o criminalización indebida, garantizando la protección de los derechos de la víctima y de la niña, niño o adolescente involucrado.

**Artículo 47. (Protocolo de prevención y protección en casos de violencia digital)**

I. El Ministerio de Educación, en coordinación con las autoridades competentes, elaborará, aprobará e implementará un Protocolo de prevención y protección en casos de violencia digital, que se adecuará a la normativa vigente y será aplicable en los niveles de educación primaria, secundaria, superior y alternativa.

El Protocolo tendrá por objeto:

- a. Establecer medidas de prevención de la violencia digital en el ámbito educativo.
- b. Definir procedimientos para la atención y protección inmediata de las víctimas.
- c. Garantizar la adopción de medidas urgentes de protección, evitando la revictimización.
- d. Establecer mecanismos de coordinación con las autoridades competentes para coadyuvar en lo que corresponda en las investigaciones administrativas, disciplinarias y judiciales, cuando los hechos se produzcan en el ámbito educativo.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

II. Las instituciones educativas, públicas y privadas, deberán aplicar obligatoriamente el Protocolo de prevención y protección en casos de violencia digital, conforme a los lineamientos que establezca el Ministerio de Educación.

**TÍTULO V: RÉGIMEN PENAL Y SANCIONES**

**CAPÍTULO I: MODIFICACIÓN E INCORPORACIONES AL CÓDIGO PENAL Y  
MODIFICACIÓN AL CÓDIGO DE PROCEDIMIENTO PENAL**

**Artículo 48. (Modificación al Código Penal).**

Se modifica el nombre del Capítulo Único del Título IX Delitos contra el Honor, de la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, con el siguiente texto:

**"CAPÍTULO PRIMERO  
DIFAMACIÓN, CAMULNIA E INJURIA"**

**Artículo 49. (Incorporaciones al Código Penal).**

I. Se incorpora a la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, el artículo 308 Quater dentro del Título XI de Delitos contra la Libertad Sexual, con el siguiente texto:

**"Artículo 308 Quater. (Violación a la intimidad sexual).**

Quien grabe, fotografíe, filme, cree, elabore o altere imágenes, audios, conversaciones o videos de contenido íntimo sexual de una persona sin su consentimiento o mediante engaño o manipulación, o quien exponga, distribuya, difunda, exhiba, reproduzca, transmita, intercambie, comparta, instigue la difusión de imágenes, audios, conversaciones o videos de contenido sexual íntimo de una persona sin su consentimiento, será sancionado con pena de privación de libertad de cuatro (4) a seis (6) años."

II. Se incorpora a la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, el artículo 323 Quinquies dentro del Título XI de Delitos contra la Libertad Sexual, con el siguiente texto:

**"Artículo 323 Quinquies. (Intimidación sexual digital).**

I. Quien intimide con difundir contenido íntimo sexual con el fin de manipular, controlar o generar daño psicológico en una persona, será sancionada con privación de libertad de dos (2) a cuatro (4) años.

II. La pena se agravará en un tercio cuando la persona amenace con difundir contenido íntimo sexual para obtener para sí o una tercera persona ventaja y/o beneficio económico, sexual u obligue a una persona a realizar actos en contra de su voluntad."

III. Se incorpora a la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, el artículo 323 Sexies dentro del Título XI de Delitos contra la Libertad Sexual, con el siguiente texto:

**"Artículo 323 Sexies. (Acoso digital).**





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

I. Quien, mediante medios digitales de forma reiterada, vigile, persiga, hostigue, intimide o busque establecer contacto sin consentimiento con una persona, será sancionado con pena de privación de libertad de dos (2) a cuatro (4) años.

II. La pena se agravará en un tercio si el acoso pasa del ámbito digital al contacto personal."

IV. Se incorpora a la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, el artículo 323 Septies dentro del Título XI de Delitos contra la Libertad Sexual, con el siguiente texto:

**"Artículo 323 Septies. (Agravantes especiales en delitos de violencia digital).**

I. Sin perjuicio de las agravantes previstas en el Código Penal, las penas establecidas para los delitos de violencia digital se incrementarán hasta en un tercio cuando concurra alguna de las siguientes circunstancias:

- a. Cuando la víctima sea autoridad electa o designada, dirigente social, sindical, comunitaria o política, o ejerza funciones de liderazgo público.
- b. Cuando la víctima sea defensora de derechos humanos, activista o líder social.
- c. Cuando la víctima sea periodista, trabajadora o trabajador de un medio de comunicación.
- d. Cuando el hecho sea cometido por la o el cónyuge, excónyuge, pareja o expareja, o por una persona con la que la víctima mantenga o haya mantenido una relación afectiva, familiar o de confianza.
- e. Cuando el contenido o las acciones de violencia digital hayan sido difundidos de forma masiva, viral o mediante el uso de múltiples plataformas digitales.
- f. Cuando la conducta sea realizada de manera coordinada, organizada o mediante financiamiento con el propósito de amplificar su difusión o impacto.
- g. Cuando, como consecuencia de la violencia digital, la víctima sufra daños físicos, sexuales, psicológicos, económicos u otros según normativa vigente.

II. Si como consecuencia directa de los hechos de violencia digital la víctima atenta contra su integridad o pierde la vida, se aplicarán las disposiciones correspondientes del Código Penal, incluyendo lo previsto en el artículo 256 relativo al homicidio-suicidio."

V. Se incorpora a la Ley N° 1768 de 10 de marzo de 1997, elevada a rango de ley mediante Decreto Ley N° 10426, de 23 de agosto de 1972, el "Capítulo Segundo Delitos contra el Honor en Entornos Digitales" con los artículos 290 Bis y 290 Ter, dentro del Título IX Delitos contra el Honor, con el siguiente texto:

**"Artículo 290 Bis: (Difusión de datos personales).**

Quien publique o difunda datos personales, información privada o información de contacto de otra persona sin su consentimiento través de medios digitales con el propósito de hostigar, intimidar o poner gravemente en riesgo su seguridad, la de su familia, entorno cercano, será sancionado con pena de privación de libertad de dos (2) a cuatro (4) años."





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**"Artículo 290 Ter. (Suplantación de Identidad Digital).**

Quien cree, utilice o manipule perfiles, cuentas o identidades digitales utilizando el nombre, imagen o datos personales de otra persona sin su consentimiento, con el propósito de causar daño, afectar su honor, reputación, seguridad, cometer actos ilícitos y/o inducir a error de forma fraudulenta, será sancionado con pena de privación de libertad de dos (2) a cuatro (4) años."

**Artículo 50. (MODIFICACIÓN AL CÓDIGO DE PROCEDIMIENTO PENAL).**

Se modifica el Artículo 282 Bis. de la Ley N° 1970, de 25 de marzo de 1999 "Código de Procedimiento Penal", modificada por la Ley N° 1636, 10 de septiembre de 2025, con el siguiente texto:

**"Artículo 282 Bis. (AGENTE ENCUBIERTO EN ENTORNOS DIGITALES).**

I. En la investigación de delitos a la vulneración de la integridad sexual de niñas, niños y adolescentes en entornos digitales, en caso de ausencia o insuficiencia de medios de prueba el Ministerio Público podrá solicitar fundadamente, bajo su responsabilidad, al Juez o la Jueza de Instrucción en lo Penal, la autorización de intervención de agentes encubiertos, en entornos digitales, de miembros de la Policía Boliviana especializados, sin antecedentes disciplinarios que presten su consentimiento al efecto.

II. Además de lo dispuesto del Artículo 282 de la presente Ley, en lo que corresponda en el marco del agente encubierto en el marco de las investigaciones, realizará actividades en entornos digitales sin que las mismas vulneren derechos de las personas y deberá informar de las mismas a la o el Fiscal que tiene a su cargo la dirección funcional de la investigación."

**CAPÍTULO II: RESPONSABILIDAD ADMINISTRATIVA DE LOS INTERMEDIARIOS DE INTERNET Y EMPRESAS DE COMUNICACIÓN**

**Artículo 51. (Responsabilidad administrativa)**

I. Los intermediarios de internet y las empresas de comunicación incurrirán en responsabilidad administrativa únicamente cuando, en el marco de la presente Ley, incumplan una orden expresa, válida y debidamente notificada, emitida por autoridad competente, de conformidad con el principio de legalidad y el debido proceso.

II. Las sanciones administrativas deberán observar los principios de razonabilidad y gradualidad, en función de la gravedad de la infracción, la reincidencia y el daño ocasionado. Estas podrán incluir multas y otras medidas correctivas, priorizando la asignación de los recursos recaudados a programas de prevención, atención y reparación integral de víctimas de violencia digital.

III. La responsabilidad administrativa prevista en el presente artículo se aplicará sin perjuicio de las responsabilidades civiles o penales que correspondan.

**Artículo 52. (Tratamiento de datos y colaboración de operadores de telecomunicaciones)**

I. Las empresas operadoras de servicios de telecomunicaciones deberán garantizar la verificación razonable de la identidad de las personas usuarias al momento de la contratación del servicio, conforme a la normativa vigente.

II. La conservación, acceso o entrega de datos personales, datos de tráfico o información asociada a las comunicaciones únicamente procederá cuando





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

medie orden judicial o requerimiento fiscal debidamente fundamentado, específico y proporcional, en el marco de una investigación.

**III.** Se prohíbe la retención masiva, indiscriminada o preventiva de datos personales, así como cualquier forma de tratamiento que vulnere los derechos a la privacidad, intimidad y secreto de las comunicaciones.

**IV.** Las empresas deberán adoptar medidas técnicas y organizativas para garantizar la seguridad, confidencialidad e integridad de los datos, evitando accesos no autorizados o usos indebidos.

**V.** El incumplimiento de obligaciones específicas establecidas mediante orden de autoridad competente dará lugar a responsabilidad conforme a la normativa vigente.

**Artículo 53. (Procedimiento administrativo sancionador)**

**I.** El procedimiento para la determinación de responsabilidades administrativas de las empresas de comunicación e intermediarios de internet deberá garantizar el debido proceso, incluyendo el derecho a la defensa, a presentar pruebas y a impugnar las decisiones.

**II.** El desarrollo específico del procedimiento será establecido en la reglamentación de la presente Ley.

**DISPOSICIONES TRANSITORIAS**

**PRIMERA.** - El Órgano Ejecutivo, a través de las entidades competentes, aprobará la reglamentación de la presente Ley en un plazo de ciento ochenta (180) días calendario desde su publicación, garantizando la participación de la sociedad civil, la academia, el sector privado y otros actores relevantes.

**SEGUNDA.** - Los intermediarios de internet y las empresas de comunicación que operen o presten servicios en el territorio del Estado Plurinacional de Bolivia deberán adecuar sus políticas, mecanismos y procedimientos de acuerdo a lo dispuesto en la presente Ley en un plazo no mayor a noventa (90) días calendario desde la aprobación de la reglamentación de la presente Ley.

**TERCERA.** - Las entidades competentes deberán implementar o adecuar mecanismos accesibles, gratuitos y especializados para la recepción, atención y seguimiento de casos de violencia digital, en un plazo no mayor a ciento ochenta (180) días calendario desde la entrada en vigencia de la presente Ley.

**CUARTA.** - En un plazo no mayor a ciento ochenta (180) días calendario de la publicación de la presente Ley, el Estado desarrollará programas de capacitación especializados dirigidos a autoridades judiciales, Ministerio Público, fuerzas de seguridad, sector educativo y demás entidades involucradas, incorporando un enfoque de derechos humanos, género e interseccionalidad, y en los casos que corresponda, la formación en la aplicación de medidas socioeducativas adaptadas a entornos digitales

**QUINTA.** El procedimiento breve y expedito para la adopción de medidas de protección digital deberá ser implementado de manera inmediata tras la entrada en vigencia de la reglamentación, garantizando su accesibilidad en todo el territorio nacional.





ASAMBLEA LEGISLATIVA PLURINACIONAL  
CÁMARA DE DIPUTADOS

**SEXTA.** En un plazo no mayor a ciento ochenta (180) días calendario a partir de la publicación de la presente Ley, el Ministerio de Gobierno, en coordinación con los ministerios e instituciones públicas competentes deberán:

- a. Crear e implementar el Observatorio Nacional de Violencia Digital.
- b. Aprobar su estructura, funcionamiento y mecanismos de coordinación interinstitucional.
- c. Diseñar e implementar un sistema unificado de recolección, sistematización y análisis de datos sobre violencia digital.

En el mismo plazo, las instituciones públicas competentes deberán adecuar sus sistemas de información, registros administrativos y mecanismos de seguimiento, incorporando indicadores específicos sobre violencia digital.

**SÉPTIMA.** - En un plazo no mayor a ciento veinte (120) días calendario a partir de la publicación de la presente Ley, el Ministerio de Educación, en coordinación con las autoridades competentes, deberá elaborar, aprobar y difundir el Protocolo de prevención y protección en casos de violencia digital.

En un plazo adicional de noventa (90) días calendario desde la aprobación del Protocolo de prevención y protección en casos de violencia digital, las instituciones educativas públicas y privadas de los niveles primario, secundario y superior deberán adecuar sus reglamentos internos, mecanismos de atención y procedimientos disciplinarios conforme a lo establecido en el protocolo de prevención y protección en casos de violencia digital.

**DISPOSICIÓN FINAL**

**ÚNICA.** - La aplicación de la presente Ley, no implicará recursos adicionales del Tesoro General de la Nación (TGN), debiendo realizarse las modificaciones presupuestarias pertinentes en el marco del Presupuesto General del Estado.

**DISPOSICIÓN DEROGATORIA Y ABROGATORIA**

**ÚNICA.** Quedan derogadas y abrogadas todas las disposiciones contrarias a la presente Ley.

Es dada en la Sala de Sesiones de la Cámara de Diputados a los...

  
Abog. W. Marcelo Solís Valencia  
DIPUTADO NACIONAL  
CH'UQUISACA  
ASAMBLEA LEGISLATIVA PLURINACIONAL