ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

LEY PARA LA PROTECCIÓN DE LAS MUJERES EN ENTORNOS DIGITALES.

DIPUTADA MAYULI ORTEGA GUZMÁN

EXPEDIENTE N. º25.927

PROYECTO DE LEY.

LEY PARA LA PROTECCIÓN DE LAS MUJERES EN ENTORNOS DIGITALES.

Expediente N°25.927

ASAMBLEA LEGISLATIVA:

La rápida expansión de las Tecnologías de la Información y la Comunicación (TIC), el desarrollo de algoritmos de distribución masiva, el uso de inteligencia artificial generativa y la masificación de las redes sociales han reconfigurado los espacios de interacción social, económica y política. Si bien la transformación digital ha abierto canales inéditos para el ejercicio de derechos, también ha catalizado la emergencia y complejización de la Violencia Digital contra las Mujeres.

La violencia digital no constituye un fenómeno aislado, fortuito ni desconectado del entorno analógico. Por el contrario, se erige como un entramado dinámico que traslada, amplifica y profundiza las desigualdades estructurales y los estereotipos de género.

En el ámbito virtual, las agresiones adquieren características técnico-operativas sumamente lesivas:

- **Efecto multiplicador y viralidad**: El entorno digital permite extender de manera exponencial el alcance de una agresión con un esfuerzo mínimo por parte del infractor, afectando la esfera personal de la víctima a escala masiva.
- **Anonimato y asimetría punitiva**: La utilización de perfiles falsos, redes privadas virtuales o cuentas automatizadas genera una percepción de impunidad para los agresores y dificulta la trazabilidad probatoria para los órganos de investigación.
- **Permanencia e indelebilidad de la huella digital**: El material lesivo difundido en la red es susceptible de ser replicado indefinidamente, sometiendo a la víctima a una revictimización continua y prolongada en el tiempo.
- **Deslocalización física e intromisión ubicua**: A diferencia de las formas tradicionales de violencia física, la agresión digital penetra el espacio privado, doméstico y personal de las mujeres sin requerir presencia corporal inmediata.

Los datos empíricos recopilados por organismos internacionales demuestran que la violencia digital posee una escala epidémica y un marcado sesgo de género. De acuerdo con las investigaciones regionales del Programa de las Naciones Unidas para el Desarrollo (PNUD), la Secretaría General Iberoamericana (SEGIB) y la Economist Intelligence Unit[1]:

Indicador / Región	Magnitud de la Violencia Digital	Fuente y Contexto Institucional
Escala Global	85% de las mujeres han experimentado o presenciado violencia en entornos virtuales.	Estudio global sobre prevalencia de violencia en línea.
América Latina y el Caribe	91% de las mujeres afirman haber sufrido o presenciado agresiones digitales.	Medición regional compilada por el PNUD (2021).
Impunidad Sistémica	1 de cada 5 usuarias habita en países donde el acoso digital no es punible efectivamente.	Informe de la Comisión de la Banda Ancha de la ONU.

[1] Violencia digital contra las mujeres: Un panorama regional | Programa De Las Naciones Unidas Para El Desarrollo
PREVENIR LA VIOLENCIA DIGITAL CONTRA LAS MUJERES EN IBEROAMÉRICA

Incidencia por Países	**México**: 22% de usuarias de internet sufren ciberacoso (INEGI 2023). **Colombia**: 60% de mujeres entre 18 y 40 años reportan acoso digital. **Honduras**: 77,8% afirman haber sido víctimas. **Chile**: 8 de cada 10 mujeres de 16 a 18 años sufren acoso sexual en redes. **Perú**: 88% de víctimas de ciberacoso son mujeres. **Paraguay**: 54,8% ha sufrido violencia telemática. **Bolivia**: 27% sufrió abuso sexual digital y 13% acoso (AGETIC 2025). **Ecuador**: 60% de niñas y adolescentes encuestadas sufrieron violencia digital y 86% reportaron amenazas de violencia sexual.	Monitoreos nacionales y reportes del PNUD, AGETIC, Ministerios de la Mujer, Plan Internacional y Organizaciones Civiles.

El diagnóstico regional visibiliza que las agresiones digitales se concentran con virulencia diferenciada en mujeres con proyección pública: periodistas, defensoras de derechos humanos, candidatas, lideresas comunitarias e investigadoras.[2]

Agresiones basadas en el desprestigio de capacidades, injurias sexistas, amenazas directas de violencia física o sexual y campañas coordinadas de desacreditación política registran patrones de recurrencia en los que un pequeño porcentaje de cuentas agresoras genera la mayoría de los contenidos tóxicos. La consecuencia directa de estas prácticas es la generación de angustia, aislamiento social y, en última instancia, la autocensura o retiro voluntario de las mujeres del debate democrático.

Históricamente, los vacíos legislativos han respondido a la falsa dicotomía entre el "espacio físico" y el "espacio virtual", asumiendo erróneamente que los daños causados a través de medios digitales carecen de entidad material o relevancia jurídica. Esta premisa ha sido superada por la doctrina constitucional contemporánea:

[2] Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión 2022
https://www.revistas.una.ac.cr/index.php/revgefedi/article/view/20973/34963

los derechos humanos reconocidos en la Constitución rigen con la misma fuerza normativa en los entornos digitales.

El Proyecto de Ley se fundamenta en las cláusulas constitucionales relativas a:

- **El Principio de Dignidad Humana**: Base ontológica del Estado Social de Derecho, quebrantada cuando la intimidad o reputación de una persona es convertida en objeto de mercantilización o escarnio público sin consentimiento.
- **El Derecho a la Integridad Personal**: Garantía contra tratos crueles, inhumanos o degradantes, aplicable a la zozobra y sufrimiento emocional provocados por el ciberacoso y la extorsión digital.
- **El Derecho a la Protección de Datos Personales y la Propia Imagen**: Facultad de cada individuo de controlar el uso, almacenamiento y divulgación de sus datos e imágenes en entornos cibernéticos.
- **El Deber de Debida Diligencia Estatal**: Obligación de los poderes públicos de adecuar las leyes penales y administrativas para prevenir, investigar y sancionar las violaciones a derechos cometidas por particulares en plataformas virtuales.

El proyecto incorpora de manera rigurosa los estándares procedentes del Derecho Internacional de los Derechos Humanos (DIDH) y el Bloque de Constitucionalidad, dando cumplimiento a los compromisos asumidos ante el Sistema Universal y el Sistema Interamericano de Derechos Humanos.

El derecho internacional ha realizado esfuerzos a través de diversos instrumentos para visibilizar y brindar parámetros en la materia. Por ejemplo, el *Sistema Interamericano de Derechos Humanos* ha desarrollado:

- **Convención de Belém do Pará**: Constituye el pilar normativo supremo en la materia. Sus artículos 1, 2 y 7 imponen a los Estados la obligación de sancionar la violencia contra la mujer tanto en el ámbito público como en el privado. El Mecanismo de Seguimiento de la Convención (MESECVI), la Comisión Interamericana de Mujeres (CIM) y ONU Mujeres han precisado en su informe especializado *Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará* (2022) que las tecnologías de la

información representan un nuevo escenario de perpetración que exige tipos penales específicos y medidas cautelares urgentes.

- **Corte Interamericana de Derechos Humanos (Corte IDH)**: En jurisprudencia constante (casos *López Soto vs. Venezuela* y *Atenco vs. México*), la Corte ha determinado que la inacción estatal ante agresiones contra mujeres genera responsabilidad internacional por incumplimiento de la debida diligencia reinforced.

El *Sistema Universal de las Naciones Unidas:*

- **CEDAW (Comité para la Eliminación de la Discriminación contra la Mujer)**: Las Recomendaciones Generales N.º 19 y N.º 35 actualizan la definición de violencia basada en el género, reconociéndola como una forma de discriminación que abarca las modalidades tecnológicas. Asimismo, la Recomendación General N.º 33 exige garantizar el acceso efectivo a la justicia mediante la superación de barreras técnicas en la recolección de pruebas digitales.

- **Relatoría Especial de la ONU sobre la Violencia contra la Mujer**: El Informe A/HRC/38/47 de 2018 conceptualiza la ciberviolencia contra las mujeres y niñas como una violación de derechos humanos que requiere marcos legislativos integrales, superando respuestas puramente reactivas o fragmentadas.

- **Resoluciones del Consejo de Derechos Humanos de la ONU**: Las Resoluciones 38/47 (2018) y 41/6 (2019) hacen un llamado formal a los Estados a prevenir el uso indebido de las tecnologías y a exigir corresponsabilidad a las empresas proveedoras de servicios digitales.

Para garantizar la viabilidad jurídica y evitar tipos penales ambiguos que vulneren el principio de tipicidad, la ley adopta la clasificación desarrollada por la Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer (Plataforma EDVAW) y la Organización de Estados Americanos (OEA):[3]

[3] Manual práctico de seguridad digital: La violencia de género en línea contra las mujeres y las niñas

Categoría Técnica	Mecanismo Tecnológico	Manifestaciones y Ejemplos Concretos
1. Violencia Sexual Digital	Captura, montaje o edición mediante Inteligencia Artificial generativa (*Deepfakes*).	Difusión no consentida de material íntimo (*sexting* secundario), *upskirting* (grabaciones bajo la falda), *downblousing* (tomas superiores de escote), *creepshots* y montaje pornográfico.
2. Ciberhostigamiento y Ciberacoso	Comunicaciones masivas, vilipendio continuado y mensajes no solicitados.	Envió no solicitado de imágenes explícitas (*cyberflashing*), comentarios misóginos repetidos, vilipendio de reputación y *slutshaming*.
3. Intrusión y Control Tecnológico	Software espía (*spyware*), geolocalización, dispositivos conectados (IoT).	Vigilancia remota no autorizada, monitoreo por GPS, hackeo de cuentas de correo y redes sociales, robo de credenciales.
4. Ataques a la Privacidad e Identidad	Extracción y divulgación masiva de archivos personales.	*Doxxing* (publicación maliciosa de dirección, teléfono o datos familiares para incitar agresiones físicas) y suplantación de identidad.

Violencia digital contra la mujer, entenderla es el primer paso para prevenirla.

5. Violencia Política y Ataques Colectivos	Campañas automatizadas (*bots*), troleo de género coordinado.	Ataques de denegación de servicio (DDoS) a sitios web feministas, campañas masivas de desprestigio contra mujeres candidatas o periodistas.

Estudios especializados confirman que más del 90% de las víctimas de la distribución no consentida de imágenes íntimas son mujeres, afectándolas de manera desproporcionada.[4]

Los tipos penales clásicos (como las injurias, calumnias, amenazas simples o chantajes) resultan dogmáticamente insuficientes para responder a la violencia digital por las siguientes razones:

- **Inadecuación del Verbo Rector**: Los delitos tradicionales no capturan la conducta de "difundir, comercializar, exhibir o manipular material íntimo reproducido en soportes digitales o generados por inteligencia artificial".
- **Desproporción en la Fijación de la Pena**: Las sanciones aplicables a los delitos contra la honra no reflejan la gravedad del impacto psicológico y la permanencia irreversible de la agresión en internet.
- **Carencia de Criterios de Evidencia Digital**: La legislación procesal ordinaria carece de reglas ágiles para la fijación, preservación de *hash* informático y custodia de datos de tráfico y contenido.

La necesidad de esta reforma ha sido ratificada por los más altos tribunales internacionales y constitucionales:

- **Tribunal Europeo de Derechos Humanos (TEDH)**: En la sentencia *K.U. vs. Finlandia* (2009), el TEDH condenó al Estado por no proteger la privacidad digital de un menor ante la publicación no autorizada de sus datos en sitios de citas. Posteriormente, en el caso *Buturaga vs. Rumanía* (2020), el TEDH dictaminó que la investigación de la violencia de género exige examinar la

[4] Violencia contra las mujeres y las niñas facilitada por tecnologías:

cibervigilancia y la intromisión digital como parte integrante del ciclo de abuso contra las mujeres.

- **Corte Constitucional de Colombia (Sentencia T-087 de 2023)**: Al examinar tutelas presentadas por mujeres periodistas víctimas de violencia digital, la Corte reconoció explícitamente el déficit normativo del Estado para combatir la violencia de género en el entorno digital y ordenó formalmente a las autoridades gubernamentales diseñar e impulsar un proyecto de ley enfocado en la prevención, protección y creación de protocolos especializados.

- **Experiencias Legislativas Exitosas**: En el ámbito iberoamericano destacan la Ley Olimpia en México (reforma a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal), la Ley N.º 27.736 (Ley Olimpia Argentina) y la Ley Reformatoria del Código Orgánico Integral Penal de Ecuador (2021) en materia de violencia sexual digital. Estas normas sirven de referente para la presente iniciativa.

De esta manera y considerando las razones antes expuestas, someto a conocimiento de la Asamblea Legislativa el presente proyecto de ley:

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA DECRETA:

LEY PARA LA PROTECCIÓN DE LAS MUJERES EN ENTORNOS DIGITALES

Expediente N°

CAPÍTULO I - DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto de la Ley

La presente ley tiene por objeto prevenir, atender, investigar, sancionar y erradicar la violencia digital y mediada por tecnologías informáticas contra las mujeres por razones de género, así como garantizar su derecho a una vida libre de violencia en el entorno virtual, resguardando su dignidad, intimidad, privacidad, honra e imagen propia.

ARTÍCULO 2.- Definición de Violencia Digital de Género

Para los efectos de esta ley, se define la Violencia Digital de Género como:

Toda acción, omisión o conjunto de conductas realizadas, instigadas, facilitadas o agravadas mediante el uso de tecnologías de la información y la comunicación (TIC), plataformas de internet, redes sociales, sistemas informáticos o herramientas de inteligencia artificial, que por razones de género cause a una mujer daño físico, psicológico, sexual, político, económico, reputacional o simbólico, o menoscabe sus derechos fundamentales, resguardando su dignidad, intimidad, privacidad, honra e imagen propia.

ARTÍCULO 3.- Manifestaciones de la Violencia Digital de Género

Constituyen manifestaciones de violencia digital de género las siguientes conductas:

- **Difusión no consentida de contenido íntimo o sexual:** Divulgar, compartir, distribuir, publicar, comercializar o exhibir imágenes, audios o videos reales de contenido sexual e íntimo de una persona sin su previo consentimiento o autorización.

- **Alteración o manipulación digital (Deepfakes pornográficos)**: La creación, edición o suplantación de la imagen o sonido de una mujer mediante el uso de Inteligencia Artificial generativa u otros recursos tecnológicos para simular actos sexuales, desnudez o conductas denigrantes sin su consentimiento.

- **Ciberacoso y persecución digital (Stalking)**: La monitorización, rastreo o acoso reiterado a través de redes sociales, mensajería o programas espías (stalkerware) que alteren el normal desarrollo de la vida de la víctima o invadan su privacidad.

- **Ciberextorsión y sextorsión:** El chantaje o amenaza de publicar o difundir material íntimo con el fin de obtener concesiones sexuales, económicas o de control relacional.

- **Invasión no autorizada de dispositivos:** La intrusión informática en teléfonos, computadoras o cuentas personales para extraer, alterar o destruir datos o comunicaciones privadas de la víctima.

- **Violencia Política de Género en Redes:** Las campañas coordinadas de desacredito, hostigamiento o difamación orientadas a inhibir o anular el ejercicio de los derechos políticos de mujeres candidatas, parlamentarias, funcionarias o lideresas comunitarias.

- **Misoginia Digital y Violencia Mediática**: La producción y transmisión de contenidos virtuales o mediáticos que inciten al odio, promuevan la discriminación de género o hagan apología de la violencia contra las mujeres.

CAPÍTULO II - DERECHOS Y ÁMBITO DE APLICACIÓN

ARTÍCULO 4.- Ámbito de protección y derecho a un entorno digital seguro

Toda mujer tiene derecho a un entorno digital seguro, en el que se garantice el respeto de su seguridad, privacidad, libertad de expresión, participación política y acceso a la justicia, así como la protección de su identidad digital, su integridad personal en los entornos tecnológicos y el resguardo de sus datos personales.

Asimismo, tiene derecho a no ser objeto de vigilancia indebida, acoso, hostigamiento, amenazas, intimidación o manipulación digital, y al pleno ejercicio de sus derechos en condiciones de igualdad y no discriminación por razones de género.

La violencia contra las mujeres comprendida en esta disposición:

a) Puede tener lugar en cualquier relación interpersonal, independientemente de que la persona presuntamente agresora haya compartido o no el mismo domicilio que la mujer.

b) Puede producirse en el ámbito comunitario y ser perpetrada por cualquier persona.

c) Puede ser perpetrada, propiciada o tolerada por el Estado o sus agentes, ya sea por la ausencia de políticas de prevención y protección, o por la falta de actuación o respuesta oportuna ante las denuncias de violencia.

Las medidas de prevención, atención, protección y respuesta contempladas en esta ley serán de aplicación en todo el territorio nacional.

ARTÍCULO 5.- Protección en la Vida Pública y Política Local

La protección frente al acoso y la violencia digital de género se extiende a mujeres que ejerzan la función pública, la política nacional o municipal.

ARTÍCULO 6- Protección de datos personales

Las mujeres tendrán derecho a la protección de sus datos personales y a oponerse a su uso o difusión no consentida, conforme a la Ley n.º 8968, y demás normativa aplicable.

ARTÍCULO 7- Atención integral y mecanismos de protección frente a la violencia digital

El Instituto Nacional de las Mujeres (INAMU), en su condición de entidad rectora en materia de igualdad y derechos de las mujeres, promoverá y coordinará, conjuntamente con el Ministerio de Justicia y Paz, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Poder Judicial, el Ministerio Público, la Defensoría de los Habitantes y los proveedores de servicios digitales, la

implementación de mecanismos de respuesta y protección dirigidos a las mujeres que enfrenten situaciones de violencia perpetradas mediante tecnologías digitales.

Estas acciones deberán desarrollarse bajo criterios de confidencialidad, no revictimización y respeto a los derechos humanos, incorporando la perspectiva de género.

Para el cumplimiento de lo dispuesto en este artículo, las instituciones y entidades participantes deberán, dentro del ámbito de sus competencias:

a) Desarrollar e implementar procedimientos de actuación que permitan recibir, atender y canalizar de manera oportuna los casos de violencia digital, así como facilitar la conservación de elementos probatorios de carácter electrónico y el acceso de las víctimas a asistencia legal, apoyo psicológico y atención social, según corresponda.

b) Disponer de canales de atención, información y acompañamiento, tanto virtuales como presenciales, que permitan a las mujeres acceder a los servicios institucionales sin importar su lugar de residencia, en condiciones de seguridad, privacidad, trato digno y ausencia de discriminación.

c) Promover programas de formación y actualización dirigidos a las personas funcionarias encargadas de la atención de estas situaciones, orientados al reconocimiento de las distintas manifestaciones de violencia digital, sus impactos diferenciados, los enfoques de género e interseccionalidad, la protección de la información personal y los derechos fundamentales de las víctimas.

d) Diseñar, desarrollar y divulgar iniciativas de prevención y educación sobre el uso seguro, consciente y responsable de las tecnologías digitales, dirigidas a niñas, adolescentes y mujeres, que permitan identificar y prevenir conductas como el hostigamiento, la sextorsión, la manipulación y otras formas de agresión en entornos digitales. Asimismo, promover en la población general la formación en competencias y alfabetización digital, procurando su incorporación en los procesos educativos y fomentando condiciones de acceso, participación y desenvolvimiento seguro de las mujeres, niñas y adolescentes en los espacios tecnológicos.

ARTÍCULO 8- Asesoría y representación legal gratuita y acompañamiento integral.

La Defensa Pública, en coordinación con el Instituto Nacional de las Mujeres (Inamu) y el Ministerio de Justicia y Paz, garantizará a las mujeres víctimas de violencia digital el acceso a servicios gratuitos de asesoría y representación legal, especializada y con perspectiva de género, durante todas las etapas del procedimiento judicial correspondiente.

Dicha representación comprenderá el acompañamiento y patrocinio letrado de las víctimas en el ejercicio de sus derechos e intereses dentro del proceso, incluyendo la posibilidad de constituirse en querellantes, ejercer la acción civil resarcitoria cuando corresponda, participar en las actuaciones procesales y formular los recursos e impugnaciones que resulten procedentes conforme al ordenamiento jurídico.

El Instituto Nacional de las Mujeres (Inamu) deberá llevar un registro de los casos atendidos y promover mecanismos de coordinación y cooperación con instituciones públicas, organizaciones de la sociedad civil y universidades públicas, a fin de facilitar a las víctimas servicios complementarios de atención psicológica, social y jurídica, que aseguren un acompañamiento integral durante el proceso de recuperación y acceso a la justicia.

ARTÍCULO 9- Prevención, atención y abordaje de la violencia digital contra las mujeres en el ámbito político

El Instituto Nacional de las Mujeres (Inamu), los partidos políticos, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) y la Defensoría de los Habitantes, en el ámbito de sus respectivas competencias, deberán desarrollar e implementar políticas, protocolos y mecanismos de cooperación interinstitucional dirigidos a prevenir, identificar, atender y brindar acompañamiento integral a las mujeres que sean objeto de violencia digital por razones de género con ocasión del ejercicio de sus derechos de participación política, ya sea en el desempeño de cargos públicos, en procesos de precandidatura o candidatura, o en cualquier otra forma de intervención en la vida política nacional.

Para el cumplimiento de este mandato, podrán promoverse, entre otras, las siguientes acciones:

a) Establecer procedimientos accesibles y confidenciales para la recepción de denuncias, la orientación y la atención de las mujeres afectadas, así como mecanismos de coordinación inmediata con las autoridades judiciales y electorales competentes, a efectos de facilitar la adopción de las medidas cautelares y de protección que correspondan, incluida la gestión de solicitudes de retiro o restricción de contenidos digitales.

b) Implementar mecanismos de observación, evaluación y seguimiento de carácter preventivo, no sancionatorio, que permitan identificar tendencias, modalidades y patrones de violencia digital, tales como ataques coordinados, expresiones de odio, campañas de desinformación y otras manifestaciones que puedan obstaculizar o menoscabar el ejercicio pleno de los derechos políticos de las mujeres. Estas actuaciones deberán respetar la privacidad, la confidencialidad y las disposiciones vigentes en materia de protección de datos personales.

c) Desarrollar mecanismos de comunicación y cooperación con las plataformas y empresas proveedoras de servicios digitales, con el propósito de agilizar la recepción y tramitación de reportes sobre contenidos presuntamente ilícitos, procurar la conservación de los elementos probatorios digitales y facilitar la colaboración con las autoridades competentes para la ejecución de las órdenes judiciales que dispongan, según corresponda, el retiro, bloqueo o desindexación de dichos contenidos.

d) Incorporar programas de formación y capacitación obligatoria, dirigidos a las estructuras de los partidos políticos, las autoridades electorales y las personas funcionarias y representantes institucionales, sobre la prevención, identificación, abordaje y atención de la violencia digital contra las mujeres por razones de género, particularmente en el contexto de los procesos políticos y electorales.

e) Establecer mecanismos y rutas interinstitucionales de atención integral, mediante la coordinación entre el Inamu, la Defensoría de los Habitantes, el Tribunal Supremo de Elecciones (TSE) y el Poder Judicial, que permitan garantizar a las mujeres afectadas el acceso oportuno a servicios de acompañamiento psicológico, asesoría y representación legal, apoyo social y asistencia técnica especializada.

ARTÍCULO 10- Deberes y responsabilidad de las personas funcionarias públicas

Las personas funcionarias públicas, en el ámbito de las atribuciones y responsabilidades propias de sus cargos, deberán actuar con debida diligencia reforzada ante cualquier manifestación de violencia digital o ejercida mediante tecnologías contra las mujeres por razones de género. Este deber comprenderá la adopción oportuna de acciones de prevención, atención, protección, investigación y, cuando corresponda, la promoción de los procedimientos dirigidos a establecer las responsabilidades respectivas y contribuir a la erradicación de estas conductas.

El incumplimiento de los deberes funcionales relacionados con la atención y protección de las mujeres víctimas de violencia digital podrá constituir falta disciplinaria grave, de conformidad con el régimen jurídico aplicable, particularmente cuando la actuación u omisión de la persona funcionaria se manifieste en alguna de las siguientes conductas:

a) Omitir la adopción de las medidas de protección, atención o comunicación a las autoridades competentes, cuando tenga conocimiento de posibles hechos de violencia digital contra una mujer y se encuentre legalmente obligada a intervenir.

b) Obstaculizar o dificultar injustificadamente el acceso de la víctima a los mecanismos institucionales de protección y justicia, desatender sus denuncias, restar importancia a los hechos comunicados o someterla a prácticas de revictimización, incluidas aquellas sustentadas en estereotipos de género, prejuicios o valoraciones de carácter moral.

c) Revelar, divulgar, sustraer, alterar o utilizar indebidamente información personal, privada, sensible o de naturaleza íntima de las víctimas, incumpliendo los deberes de confidencialidad, seguridad y protección de datos personales establecidos en la legislación vigente, particularmente en la Ley n.º 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.

d) Realizar, promover, facilitar o participar, directa o indirectamente, en actos de violencia digital contra mujeres que se encuentren bajo su autoridad, subordinación, tutela o vinculación institucional, incluyendo conductas de hostigamiento, acoso, divulgación no consentida de material íntimo u otras acciones que lesionen sus derechos fundamentales.

Las conductas señaladas darán lugar a las responsabilidades administrativas, civiles o penales que correspondan, según la naturaleza de los hechos y de conformidad con el ordenamiento jurídico costarricense. La determinación de las sanciones deberá efectuarse mediante los procedimientos legalmente establecidos, con observancia del debido proceso y del derecho de defensa.

El Instituto Nacional de las Mujeres (Inamu), en el ejercicio de sus competencias como ente rector en materia de igualdad y equidad de género, promoverá y coordinará con las instituciones públicas la elaboración e implementación de protocolos de actuación institucional y programas permanentes de capacitación obligatoria en materia de violencia digital contra las mujeres, perspectiva de género y derechos humanos en entornos tecnológicos.

Estas acciones deberán orientarse a fortalecer las capacidades institucionales de prevención, detección y atención de estas manifestaciones de violencia, evitar prácticas de violencia institucional y asegurar el cumplimiento efectivo de los deberes funcionales establecidos en esta ley.

CAPÍTULO III - PROCESOS JUDICIALES Y GARANTÍAS PROCESALES

ARTÍCULO 11- Principios rectores para la tramitación de procesos relacionados con violencia digital.

Además de los principios, derechos y garantías reconocidos en la Constitución Política y en la legislación procesal vigente, las actuaciones judiciales relacionadas con hechos de violencia digital contra las mujeres deberán observar los siguientes principios especiales:

a) **Debida diligencia reforzada en entornos digitales:** Las autoridades competentes deberán intervenir de manera oportuna, diligente y expedita, considerando las características particulares de los medios tecnológicos, especialmente la rapidez con que se difunden los contenidos digitales, su posible modificación, reproducción o eliminación y el riesgo de que estas circunstancias dificulten la protección de las víctimas y la obtención de elementos probatorios.

b) **Integridad y eficacia de la prueba digital:** La identificación, obtención, recopilación, conservación, análisis y valoración de los elementos probatorios de

naturaleza digital deberán efectuarse mediante procedimientos técnicos adecuados, que permitan garantizar su autenticidad, integridad, trazabilidad y disponibilidad, de conformidad con los protocolos aplicables y los estándares técnicos reconocidos.

c) **Confidencialidad y protección de la identidad y los datos personales:** Las autoridades deberán adoptar las medidas necesarias para resguardar la identidad de las mujeres afectadas y proteger la información personal, privada, sensible o íntima incorporada a las actuaciones judiciales, evitando su divulgación, acceso o utilización indebida, de conformidad con la legislación vigente.

d) **Prevención de la revictimización en el ámbito judicial y digital:** Durante la tramitación de los procedimientos se evitará la exposición, reproducción o difusión innecesaria de imágenes, grabaciones, mensajes o cualquier otro material de carácter íntimo, humillante o degradante relacionado con la víctima. Asimismo, deberán adoptarse las medidas procesales necesarias para impedir que las actuaciones judiciales generen nuevas afectaciones a su dignidad, intimidad e integridad personal.

e) **Perspectiva de género e interseccionalidad:** Las autoridades judiciales deberán incorporar la perspectiva de género y el enfoque interseccional en la tramitación de los procedimientos y en el análisis de los elementos probatorios, considerando las relaciones desiguales de poder, los estereotipos de género, las manifestaciones de violencia simbólica y las particularidades de las agresiones perpetradas mediante tecnologías digitales, así como las condiciones específicas de vulnerabilidad que puedan concurrir en las mujeres afectadas.

ARTÍCULO 12- Medidas cautelares y de protección inmediata

Cuando existan elementos que permitan presumir razonablemente que una mujer se encuentra en una situación de violencia digital, las autoridades judiciales competentes, podrán disponer, de oficio o a instancia de la persona afectada o del Instituto Nacional de las Mujeres (Inamu), las medidas cautelares y de protección que resulten necesarias para salvaguardar su integridad y prevenir la continuidad de las conductas lesivas.

Para tales efectos, podrán adoptarse, entre otras, las siguientes disposiciones:

a) Ordenar a las empresas proveedoras de servicios digitales e intermediarios de internet que procedan, de manera inmediata y en un plazo máximo de veinticuatro a cuarenta y ocho horas desde su notificación por canales electrónicos oficiales, a retirar, restringir, inhabilitar temporalmente el acceso o desindexar las publicaciones, archivos o cualquier contenido digital constitutivo de violencia, sin perjuicio del deber de conservar la evidencia digital y los metadatos correspondientes. En el caso de plataformas internacionales sin representación legal en el país, el Poder Judicial y la PRODHAB habilitarán un registro de enlace y mecanismos expeditos de notificación directa, reservando la vía del auxilio judicial internacional para la obtención de datos de tráfico o identificación penal.

b) Disponer que la persona presuntamente responsable se abstenga de establecer cualquier tipo de comunicación, acercamiento o interacción con la víctima, ya sea por medios digitales, redes sociales, dispositivos electrónicos o de forma presencial.

c) Instruir la restricción o suspensión del acceso a perfiles, cuentas, servicios, plataformas o dispositivos tecnológicos que estén siendo utilizados como instrumentos para ejecutar actos de violencia digital, hostigar a la víctima o divulgar contenido ilícito. En el caso de las empresas proveedoras de servicios digitales internacionales, la solicitud de la información se debe gestionar por medio del trámite internacional legal correspondiente.

d) Establecer cualquier otra disposición de protección que resulte idónea y necesaria para impedir la prolongación de las conductas violentas, prevenir nuevas afectaciones y evitar la revictimización, de conformidad con los principios de legalidad, necesidad, proporcionalidad y tutela judicial efectiva.

El Poder Judicial deberá establecer un protocolo de actuación para la tramitación y ejecución expedita de las medidas contempladas en este artículo. Para su elaboración e implementación, deberá promover la coordinación interinstitucional con las empresas proveedoras de servicios tecnológicos, las autoridades competentes en materia de ciberseguridad y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt).

ARTÍCULO 13- Consecuencias jurídicas por el incumplimiento de las medidas cautelares o de protección

El desacato, ya sea total o parcial, de las medidas cautelares o de protección ordenadas al amparo del artículo anterior podrá generar responsabilidad penal por el delito de desobediencia a la autoridad, de conformidad con lo dispuesto en el artículo 314 del Código Penal, sin perjuicio de las demás responsabilidades que puedan derivarse de los actos de violencia digital que motivaron su imposición.

En caso de que la persona a quien se haya impuesto una medida de protección en favor de una mujer víctima de violencia digital incumpla las disposiciones ordenadas, el órgano jurisdiccional que conozca del asunto deberá poner los hechos, sin dilación, en conocimiento del Ministerio Público, para que este valore el inicio de la investigación penal correspondiente.

La reiteración de conductas prohibidas, el restablecimiento de comunicaciones por medios digitales o la divulgación ulterior del contenido cuyo acceso o difusión haya sido restringido podrán considerarse elementos relevantes para determinar la existencia de una conducta dolosa, conforme a las reglas aplicables en materia probatoria.

Lo anterior se establece sin perjuicio de las responsabilidades administrativas o disciplinarias que puedan exigirse cuando la persona infractora tenga la condición de funcionaria pública, de acuerdo con el régimen de responsabilidad y las disposiciones legales y reglamentarias aplicables.

ARTÍCULO 14- Justicia restaurativa y reparación integral de las víctimas

Los mecanismos de justicia restaurativa podrán aplicarse en los casos de violencia digital contra las mujeres únicamente cuando las características y circunstancias particulares de los hechos permitan su utilización, siempre que se cumplan de manera concurrente las siguientes condiciones:

a) Que la naturaleza de la conducta y las circunstancias del caso sean compatibles con los fines y presupuestos de la justicia restaurativa.

b) Que la víctima manifieste su voluntad de participar mediante un consentimiento libre, voluntario, previo e informado, sin que medie coacción, intimidación, presión o condicionamiento alguno.

c) Que no concurran relaciones de poder, dependencia, subordinación o cualquier otra circunstancia que pueda comprometer la libertad de decisión de la víctima o generar condiciones de desigualdad que afecten su participación en el procedimiento.

d) Que los hechos no involucren a personas menores de edad ni correspondan a conductas de especial gravedad, particularmente aquellas relacionadas con sextorsión, elaboración o utilización de representaciones sexuales falsas o manipuladas mediante tecnologías digitales (deepfakes sexuales), o divulgación no consentida de material íntimo que produzca una afectación grave a los derechos de la víctima.

Los procedimientos de justicia restaurativa que resulten legalmente procedentes deberán observar las siguientes disposiciones:

1. Su tramitación, dirección y supervisión corresponderán exclusivamente a las autoridades competentes del Poder Judicial, de conformidad con la Ley sobre Resolución Alterna de Conflictos y Promoción de la Paz Social, Ley N°7727 y su normativa reglamentaria, así como con las disposiciones especiales aplicables en materia de justicia restaurativa.

2. Las medidas restaurativas podrán comprender, según las particularidades del caso y con respeto a la voluntad de la víctima, acciones de reparación simbólica, ofrecimiento voluntario de disculpas, compromisos verificables de no repetición y otras medidas dirigidas a reparar las consecuencias de la violencia ejercida, de conformidad con la Ley de Justicia Restaurativa, Ley N°9582. Asimismo, podrá contemplarse la eliminación o restricción de acceso al contenido digital relacionado con los hechos, siempre que exista autorización de la autoridad judicial competente y se garantice previamente la preservación de los elementos probatorios necesarios.

3. La aplicación de mecanismos restaurativos no podrá utilizarse para suspender, revocar o sustituir las medidas cautelares y de protección que hayan sido dispuestas en favor de la víctima, ni limitar las potestades de las autoridades judiciales para ordenar la conservación de evidencia digital, el retiro de contenidos o cualquier otra medida necesaria para proteger sus derechos.

4. La participación de la víctima en estos procedimientos será estrictamente voluntaria y su decisión de no participar, retirarse o no alcanzar un acuerdo no podrá generar consecuencias desfavorables para ella ni afectar su derecho de acceso a la justicia.

El Instituto Nacional de las Mujeres (Inamu), el Ministerio de Justicia y Paz y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt), en el ámbito de sus respectivas competencias, podrán impulsar programas de prevención mediante iniciativas de alfabetización digital, ciudadanía responsable, educación en igualdad de género y promoción de relaciones respetuosas en los entornos tecnológicos. Estas instituciones no podrán asumir funciones de dirección, facilitación o resolución de los procedimientos judiciales de justicia restaurativa.

CAPÍTULO IV - REFORMAS DE OTRAS LEYES

ARTÍCULO 15- Modificación de la Ley N.º 10235, Ley para Prevenir, Atender, Sancionar y Erradicar la Violencia contra las Mujeres en la Política

Se adicionan las siguientes disposiciones a la Ley N.º 10235, Ley para Prevenir, Atender, Sancionar y Erradicar la Violencia contra las Mujeres en la Política:

ARTÍCULO 3- Ámbito de aplicación de esta ley. Esta ley protege los derechos de las mujeres a una vida libre de violencia de género en la política y será de aplicación en los siguientes ámbitos:

a) Cuando las mujeres sean afiliadas y participen en la estructura, comisiones u órganos a lo interno de los partidos políticos.

b) Cuando las mujeres sean aspirantes, precandidatas y candidatas a cargos de elección popular o de designación.

c) Cuando las mujeres estén en el ejercicio de cargos de elección popular, o de designación.

d) Cuando, por la naturaleza de sus funciones, las mujeres estén a cargo de la promoción y ejecución de políticas públicas institucionales de igualdad de género y derechos políticos de las mujeres, y participen en órganos, programas y estructuras en instituciones públicas para el cumplimiento de sus competencias y atribuciones.

e) Cuando las mujeres sean objeto de acciones de violencia política de género en entornos digitales, incluyendo campañas coordinadas de ciberacoso, ataques organizados mediante brigading, granjas de troles, cuentas automatizadas o mecanismos similares, dirigidos a intimidar, desacreditar, silenciar, excluir u obstaculizar su participación o el ejercicio de sus derechos políticos, en el ámbito nacional o municipal, independientemente de que dichas acciones sean ejecutadas por una o varias personas, mediante cuentas reales, falsas o automatizadas.

Artículo 4 bis- Violencia político-digital

Para efectos de esta ley, se reconoce la violencia político-digital como una manifestación de violencia contra las mujeres en el ámbito político, ejercida mediante tecnologías de la información y la comunicación, redes sociales, plataformas digitales o cualquier otro medio tecnológico, cuando tenga por objeto o resultado obstaculizar, restringir, menoscabar o impedir el ejercicio de sus derechos políticos, su participación en la vida democrática o el desempeño de cargos y funciones públicas, por razones de género.

Artículo 21 bis- Medidas de protección digital de carácter urgente

Cuando se denuncien hechos de violencia político-digital durante procesos de precandidatura, campañas electorales, procesos de elección o designación, o durante el ejercicio de cargos públicos, las autoridades judiciales competentes podrán disponer, con carácter urgente y mediante resolución debidamente fundamentada, las medidas de protección digital que resulten necesarias y proporcionales para salvaguardar los derechos de las mujeres afectadas.

La solicitud de estas medidas deberá recibir tramitación prioritaria, de manera que la autoridad competente procure resolverla dentro de un plazo máximo de cuarenta y ocho horas, atendiendo a las circunstancias particulares y al riesgo de continuidad o agravamiento del daño.

Entre las medidas que podrán ordenarse se encuentran:

a) Requerir la desindexación de publicaciones o contenidos digitales cuya difusión constituya una manifestación de violencia político-digital, cuando concurran los presupuestos legales para ello.

b) Disponer el retiro o la restricción temporal de acceso a publicaciones, imágenes, grabaciones u otros materiales digitales que vulneren los derechos de la víctima.

c) Ordenar, cuando resulte técnicamente viable y jurídicamente procedente, la restricción geográfica del acceso a determinados contenidos.

d) Disponer la conservación y preservación de los contenidos y demás elementos digitales que puedan constituir prueba de los hechos denunciados.

e) Adoptar cualquier otra medida de protección digital que resulte idónea, necesaria y proporcional para prevenir la continuidad de las agresiones o evitar nuevas afectaciones.

La tramitación y ejecución de estas medidas deberá observar los principios de debida diligencia reforzada, protección de los derechos políticos de las mujeres, perspectiva de género, proporcionalidad y tutela judicial efectiva, sin menoscabo de las garantías constitucionales y procesales aplicables.

ARTÍCULO 16- Reforma de la Ley N.º 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales

Se adicionan las siguientes disposiciones a la Ley N.º 8968 Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales:

Artículo 7 bis- Procedimiento expedito ante la PRODHAB y el Poder Judicial. Las mujeres afectadas por la divulgación no consentida de material íntimo, la utilización de representaciones sexuales manipuladas digitalmente, la suplantación de identidad mediante tecnologías digitales o cualquier otra modalidad de tratamiento ilícito de sus datos personales que constituya violencia digital podrán solicitar, ante la Agencia de Protección de Datos de los Habitantes (PRODHAB) o el órgano judicial competente, la aplicación de un procedimiento expedito para la desindexación y supresión de contenidos en un plazo de cuarenta y ocho horas.

Artículo 13 bis- Red de Cooperación Interinstitucional.

La PRODHAB mantendrá un registro actualizado de los oficiales de privacidad y canales de enlace de las plataformas digitales operantes en el país para la ejecución expedita de medidas de tutela de datos personales.

ARTÍCULO 17- Reforma del Código Penal, Ley N.º 4573

Se adicionan los siguientes artículos al Código Penal, Ley N°4573:

Artículo 196 ter - Difusión no consentida de material íntimo o sexual

Será sancionada con pena de prisión de uno a cuatro años la persona que, sin el consentimiento libre e informado de quien aparece en el material, divulgue, publique, transmita, comparta o ponga a disposición de terceras personas imágenes, grabaciones de audio o video u otros registros de naturaleza íntima o sexual.

La pena será de dos a cinco años de prisión si:

a) Se realiza con propósito de lucro;

b) La víctima es menor de edad o persona con discapacidad;

c) Se ejecuta mediante suplantación de identidad;

d) Se causa un daño grave a la integridad física o mental de la víctima.

Artículo 196 quater- Divulgación ilícita de datos personales con finalidad de intimidación o exposición al riesgo

Será sancionada con pena de prisión de uno a tres años la persona que, sin autorización y con la finalidad de intimidar, hostigar, amenazar o exponer a una mujer a un peligro concreto, divulgue, publique o facilite a terceras personas datos personales de carácter privado, restringido o sensible, cuando dicha conducta genere un riesgo real para la seguridad, integridad personal o tranquilidad de la víctima o su grupo familiar.

Artículo 198 bis- Representaciones sexuales manipuladas o simuladas

Será sancionada con pena de prisión de dos a seis años la persona que, mediante inteligencia artificial, software de edición o cualquier recurso tecnológico, genere, altere, modifique o simule imágenes, grabaciones de audio o video, o cualquier representación digital de naturaleza sexual que atribuya falsamente a una mujer su participación en actos de contenido sexual, y las divulgue, publique, comercialice o ponga a disposición de terceros sin su consentimiento.

Artículo 198 ter.- Cláusula de Especialidad y Subsidiariedad.

Los delitos contemplados en los artículos 196 ter, 196 quater, 198 bis, 214 ter y 388 ter de este Código se aplicarán de forma subsidiaria, salvo que la conducta configure una modalidad de violencia sancionada con una pena mayor en la Ley de Penalización de la Violencia contra las Mujeres (Ley N.º 8589) o la Ley de Protección de la Niñez y Adolescencia.

Artículo 214 ter- Extorsión mediante amenazas de divulgación de contenido íntimo o información personal

Será sancionada con pena de prisión de tres a siete años la persona que, mediante la amenaza de divulgar, publicar o revelar material íntimo, datos personales o información de naturaleza privada o degradante, obligue a una mujer a realizar, tolerar u omitir una conducta, efectuar una disposición patrimonial o entregar dinero, bienes o cualquier otro beneficio.

La pena será de cuatro a diez años de prisión cuando concurra alguna de las siguientes circunstancias:

a) Que la víctima sea menor de edad, sin perjuicio de las disposiciones penales especiales aplicables.

b) Que la conducta se ejecute mediante campañas coordinadas, utilización de múltiples cuentas o mecanismos de difusión masiva destinados a incrementar la intimidación o presión sobre la víctima.

Artículo 388 ter- Ciberacoso u hostigamiento digital.

Quien, mediante acciones reiteradas en entornos digitales, cause intimidación, degradación, hostigamiento o perturbación grave a una mujer, será sancionado con prisión de seis meses a dos años, cuando la conducta sea idónea para afectar gravemente su integridad o tranquilidad personal.

La pena será de uno a tres años si:

a) la agresión es colectiva (bots, brigadas digitales),

b) la víctima es periodista, funcionaria pública o defensora de derechos humanos,

c) existe motivación de género.

ARTÍCULO 18- Reforma de la Ley N° 7801, Ley del Instituto Nacional de las Mujeres.

Adiciónese un nuevo inciso al artículo 4 de la Ley N.º 7801, para que se lea:

"NUEVO INCISO": Garantizar patrocinio letrado, representación judicial gratuita y acompañamiento integral a las mujeres víctimas de violencia digital."

CAPÍTULO V - DISPOSICIONES TRANSITORIAS

TRANSITORIO I- Reglamentación

El Poder Ejecutivo deberá emitir el reglamento necesario para la implementación y ejecución de las disposiciones contenidas en esta ley, dentro del plazo máximo de seis meses.

La ausencia de reglamentación no impedirá la aplicación de aquellas disposiciones de esta ley que sean susceptibles de ejecución directa.

Rige a partir de su publicación.

MAYULI ORTEGA GUZMÁN

DIPUTADA