ASAMBLEA LEGISLATIVA DE LA

REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

LEY PARA PREVENIR, ATENDER, PROTEGER, INVESTIGAR, SANCIONAR Y ERRADICAR LA VIOLENCIA DIGITAL CONTRA LAS MUJERES POR RAZONES DE GÉNERO; y REFORMA DE LOS ARTÍCULOS 3 y 9 BIS DE LA LEY N.º 10235; LOS ARTÍCULOS 7 Y 20 DE LA LEY N.º 8968; Y LOS ARTÍCULOS 152, 196, 196 BIS, 196 TER, 196 QUATER Y 196 QUINQUIES DE LA LEY N.º 4573

DIPUTADAS

Cynthia Córdoba Serrano **Luz Mary Alpízar Loaiza**

y otros diputados

EXPEDIENTE N.º25.322

2025

PROYECTO DE LEY

LEY PARA PREVENIR, ATENDER, PROTEGER, INVESTIGAR, SANCIONAR Y ERRADICAR LA VIOLENCIA DIGITAL CONTRA LAS MUJERES POR RAZONES DE GÉNERO; REFORMA DE LOS ARTÍCULOS 3 y 9 BIS DE LA LEY N.° 10235; LOS ARTÍCULOS 7 Y 20 DE LA LEY N.° 8968; Y LOS ARTÍCULOS 152, 196, 196 BIS, 196 TER, 196 QUATER Y 196 QUINQUIES DE LA LEY N.° 4573

Expediente N.º25.322

La digitalización de la vida social, política y económica ha creado nuevos espacios donde la violencia online (en línea) contra las mujeres se manifiesta mediante conductas como el acoso digital, la captura y difusión no consentida de imágenes íntimas, la suplantación de identidad, la manipulación algorítmica discriminatoria y los discursos de odio. Estas acciones, presentes en redes sociales, correos electrónicos, aplicaciones o cualquier otro medio digital, buscan vulnerar la dignidad, la seguridad, la privacidad y la libertad de las mujeres involucradas.

La agresión ejercida en entornos digitales se entrelaza con la violencia machista que afecta cotidianamente a mujeres y niñas en espacios públicos, laborales e incluso dentro de sus hogares o círculos afectivos. No existe una frontera entre lo que ocurre en línea y lo que sucede fuera de ella; ambas dimensiones forman parte de la misma realidad y generan impactos igualmente graves en la vida de quienes lo sufren. Las plataformas digitales simplemente operan como nuevos escenarios dentro del mismo entramado estructural de desigualdad entre hombre y mujeres; un continuo de la violencia.

La violencia digital contra las mujeres constituye una modalidad cada vez más común y dañina de agresión que, empleando entornos digitales, atenta contra el derecho de las mujeres a una vida libre de violencia, reconocido por el artículo 50 de la Constitución Política de Costa Rica, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Belém do Pará), la CEDAW y la Ley de Penalización de la Violencia Contra las Mujeres N.° 8589.

En los últimos años, Costa Rica ha registrado un incremento sostenido de denuncias por violencia digital, particularmente entre mujeres menores de 35 años, funcionarias públicas y adolescentes. Esto incluye formas graves como difusión no consentida de contenido íntimo, “deepfakes” sexuales, sextorsión, hostigamiento masivo en redes, persecución digital y doxing, afectando su privacidad, intimidar y

su libertad de participación social y política, y por supuesto, afectando su salud mental y su integridad personal.

Costa Rica carece actualmente de una legislación específica sobre violencia digital con perspectiva de género. Si bien leyes como la Ley N.º 10235 sobre violencia política contra las mujeres y la Ley N.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales contienen disposiciones relevantes, no existe un marco único, específico y articulado que aborde de forma integral esta problemática.

A nivel internacional, países como México (Ley Olimpia, 2021), Australia (Online Safety Act, 2021), Reino Unido (Online Safety Act, 2023) y la Unión Europea (DSA, 2024) han implementado leyes o normativas sólidas que castigan la violencia digital, protegen los datos personales, regulan comportamientos tecnológicos y responsabilizan a plataformas digitales en la prevención y eliminación de contenido violento y degradante. Costa Rica debe avanzar en esta dirección, con un enfoque nacional contextualizado y una construcción legal con perspectiva de género, derechos humanos y democracia.

País	Norma o Ley	Año	Aspectos más relevantes
México	Reforma conocida como “Ley Olimpia”	2021	Reconoce la violencia digital y penaliza la difusión íntima no consentida
Australia	Online Safety Act	2021	Obliga a remover contenido dañino en 24 horas y protege contra “deepfakes”
Reino Unido	Online Safety Act	2023	Crea deber de cuidado para plataformas ante contenido dañino a grupos protegidos
Brasil	Ley Carolina Dieckmann	2012	Penaliza delitos informáticos y difusión privada sin consentimiento
Argentina	Ley Mica Ortega	2020	Incluye herramientas de prevención educativa contra grooming digital
Unión Europea	Reglamento de Servicios Digitales (DSA)	2024	Establece obligaciones a plataformas según su tamaño e impacto sistémico

Adicionalmente, la ONU Mujeres (2023) explica y ejemplifica este tipo de violencia de la siguiente manera[1]:

Nombre	Definición	Ejemplos
Amenazas directas de daño o violencia	Implica el envío o publicación de comunicaciones o contenidos digitales que le anticipan a una persona la intención de cometer en su contra un daño físico o violencia sexual, o en contra de sus familiares, amistades o bienes.	Incluye actos como extorsión digital, que involucra el uso de las tecnologías de la información y la comunicación (TIC) para ejercer presión sobre una persona a fin de forzarla a actuar de cierto modo u obtener dinero y/o amenazas de difundir o enviar a familiares de la víctima información privada para su explotación o chantaje sexual.
Violencia física facilitada por las nuevas tecnologías	Esta forma de violencia conlleva el uso de las TIC para ubicar y acceder a una víctima a fin de agredirla física o sexualmente.	Algunas de las conductas que involucran son agresiones físicas como consecuencia de actos de doxeo, ataques sexuales organizados o planificados mediante el uso de las TIC, entablar amistad en redes sociales o sitios de citas para abuso sexual o feminicidios/feminicidios y/o obligar a una persona a entablar relaciones sexuales bajo amenaza de publicar información íntima o sexual (sextorsión).
Explotación sexual y/o trata de mujeres y niñas facilitada por las tecnologías	Esta forma de violencia conlleva la intermediación de las tecnologías para el ejercicio de poder sobre una víctima con el objeto de cometer abuso o explotación sexual de su	Puede involucrar el grooming y el uso de la TIC para la selección y el engaño de víctimas con fines de abuso sexual o trata de mujeres y niñas.

[1] https://documents.un.org/doc/undoc/gen/n24/288/17/pdf/n2428817.pdf

Nombre	Definición	Ejemplos
	imagen y/o de su cuerpo contra su voluntad.	
Ataques a grupos, organizaciones, comunidades o colectivas de mujeres	Involucran acciones intencionales para censurar y/o causar daño a organizaciones o grupos de mujeres, para afectar el desarrollo de sus funciones, atacar sus canales de expresión, intimidarlas para retirar publicaciones o silenciarlas y disminuir o anular su presencia en los espacios y conversaciones digitales.	Estos ciberataques pueden involucrar el hackeo de sitios web, cuentas de redes sociales o cuentas de correo electrónico, y/o actos para dañar el perfil de redes sociales mediante el uso de normas comunitarias reportando de forma masiva contenido que se considera sensible (bloqueos, páginas o perfiles de la organización).
Acceso no consentido y/o ataque a la integridad de un sistema informático o a una cuenta en línea, así como el uso, control, manipulación o publicación no autorizada de información privada y datos personales	Se configura mediante el acceso no autorizado o hackeo a las cuentas en línea o dispositivos electrónicos de una mujer para controlarlos y/o obtener y manipular información o datos personales o para publicarlos sin consentimiento, como una forma de intimidación o humillación o con el objetivo de generar daños y afectaciones a la víctima de diversa índole en su psiquis y en su entorno social.	Puede incluir uso, manipulación y modificación no consentida de información (eliminar, modificar o falsificar datos personales, incluyendo fotos y videos).
Suplantación y robo de identidad en línea	Consiste en la utilización de la imagen, información o datos de una persona o la creación de una identidad falsa con la imagen o datos de una	Creación de perfiles o cuentas falsas en redes sociales o de cuentas de correo electrónico que utilizan la información o imagen de una persona u organización y/o robo de dinero o realizar compras

Nombre	Definición	Ejemplos
	persona, sin mediar su consentimiento y a través del uso de las TIC, con el fin de amenazar, intimidar o dañar su reputación.	en línea a partir del robo de datos bancarios.
Actos que implican monitoreo, control y vigilancia en línea	Esta forma de violencia digital consiste en el rastreo constante de las actividades en línea y fuera de línea de una víctima, así como de su ubicación, desplazamientos e información a través del uso de las TIC.	Utilización de software espía en dispositivos electrónicos, sin el consentimiento de la usuaria, que permiten el control remoto de cámaras o micrófonos en teléfonos móviles, o el monitoreo calendarizado de llamadas y mensajes y/o instalación y/o uso de aplicaciones para monitorear las actividades en línea, incluyendo aplicaciones de "control parental".
Ataques a la reputación o credibilidad	Implica la creación, manipulación y publicación de información personal falsa, manipulada o fuera de contexto con la intención de descalificar o dañar la reputación de una persona o que puede implicar un daño a su trayectoria, credibilidad o imagen pública.	Creación de perfiles falsos en redes sociales o cuentas en línea con la intención de afectar la reputación de la víctima y/o publicar avisos de publicidad falsos en sitios de citas o pornográficos.

Basado en lo anterior, es posible comprender que la violencia digital contra mujeres y niñas no solo genera daño emocional, físico, sexual o económico, sino que también limita su capacidad de participar plenamente en la sociedad. Estas agresiones pueden hacer que muchas mujeres se alejen de espacios públicos, debates y actividades en línea por miedo o agotamiento, lo que afecta su bienestar, sus oportunidades y su desarrollo personal y profesional, entre otros derechos fundamentales como la libertad de expresión y una vida libre de violencia en todos los ámbitos.

La investigación internacional advierte además que las TIC, cuando carecen de mecanismos eficaces de moderación y protección, pueden contribuir a normalizar y trivializar conductas violentas, reforzando estereotipos y permitiendo la reproducción sistemática de violencia simbólica, psicológica y sexual en formatos digitales.

El más reciente Informe sobre Discursos de Odio y Discriminación 2025 de Naciones Unidas evidencia una realidad alarmante para Costa Rica[2]. Advierte que no solo hay más contenido de odio, sino también más personas generándolo. El número de individuos que emiten mensajes discriminatorios en redes sociales aumentó en un 31%, con expresiones cada vez más agresivas, personalizadas y provenientes mayoritariamente de cuentas reales.

Dicho informe destaca el papel de las masculinidades agresivas en la reproducción de violencia digital: siete de cada diez mensajes de odio son emitidos por hombres, evidenciando patrones culturales persistentes que normalizan la misoginia y la agresividad como formas de interacción social. Además, las agresiones dirigidas hacia las mujeres muestran una tendencia sostenida al alza. Solo en 2025 se registraron 491 mil mensajes contra lideresas, activistas, defensoras de derechos humanos y mujeres que enfrentan violencia.

Esta situación también se evidencia en la investigación "Violencia digital contra mujeres en el ejercicio profesional de la comunicación", desarrollada el Colegio de Periodistas y Profesionales en Ciencias de la Comunicación Colectiva de Costa Rica (Colper) y el Centro de Investigación en Comunicación (CICOM) de la Universidad de Costa Rica (UCR), quienes entrevistaron a 116 comunicadoras con representación de todas las provincias del país, de las cuales el 23,1% señalaron haber sufrido violencia digital en el 2024, frente a 23,3% en el 2023. El 39% de comunicadoras que sufren violencia digital aceptaron que se autocensuran para evitar más ataques.

Por su parte, ONU Mujeres estima que, a escala global, el 73% de las mujeres ha estado expuesta o ha sufrido algún tipo de agresión en línea. Además, el 23% reporta haber experimentado abuso o acoso digital al menos una vez en su vida y se calcula que una de cada diez mujeres a partir de los 15 años ha sido víctima de violencia en entornos digitales. A ello se suma un dato particularmente alarmante: el 90% de las personas afectadas por la difusión no consentida de imágenes íntimas son mujeres.

[2] https://costarica.un.org/es/299679-informe-sobre-discursos-de-odio-y-discriminaci%C3%B3n-2025

Estas cifras dan cuenta de un fenómeno extendido y profundamente desigual, que exige respuestas firmes y coordinadas para garantizar la seguridad y la dignidad de las mujeres en los espacios digitales.

Pese a avances normativos como la adhesión al Convenio de Budapest sobre Ciberdelincuencia (2017) y a la Declaración de la Red Iberoamericana de Protección de Datos (2021), el Código de la Niñez y la Adolescencia (Ley 7739), la Ley contra el acoso escolar (Ley 9404), la reforma al Código Penal que incluye el espionaje informático (Ley N.º 9048), Ley contra el hostigamiento o acoso sexual en el empleo y la función pública (Ley N.º 9967), la Ley contra el Acoso Sexual Callejero (Ley 9877),la Ley para Prevenir, Atender, Sancionar y Erradicar la Violencia contra las Mujeres en la Política (Ley 10235) y la Ley contra el acoso predatorio (Ley 10.487), entre otros, aún persisten vacíos significativos que impiden una respuesta integral, oportuna y efectiva frente a la violencia de género en línea, y como tal, Costa Rica no cuenta con una ley específica contra la violencia digital.

En este contexto, el presente proyecto de Ley tiene el objetivo de fortalecer la protección de los derechos humanos de las mujeres frente a las manifestaciones de violencia digital o mediada por tecnologías, pues reconoce que la violencia de género en línea no solo replica los patrones históricos de discriminación y subordinación hacia las mujeres, sino que también los magnifica a través de la velocidad, alcance y persistencia que permiten los entornos digitales.

Esta propuesta busca armonizar el marco nacional con la Ley Modelo Interamericana de la OEA, incorporando medidas preventivas, de atención, investigación, protección, reparación y sanción, así como mecanismos de coordinación interinstitucional y regulación de proveedores digitales bajo principios de debida diligencia, igualdad y derechos humanos.

Asimismo, tiene este proyecto de ley tiene vinculación con los siguientes Objetivos de Desarrollo Sostenible (ODS):

ODS 4 (Educación de Calidad): alfabetización digital con enfoque de género (arts. 24–25).

ODS 5 (Igualdad de Género): erradicar la violencia contra mujeres y niñas (arts. 1, 4–6, 8–12, 23–26).

ODS 9 (Innovación e Infraestructura): responsabilidad y transparencia de plataformas (arts. 13–20)

ODS 16 (Paz, Justicia e Instituciones Sólidas): acceso a justicia y debida diligencia (arts. 7–13, 21–22, 26).

Por las siguientes razones:

El ODS 4: Educación de Calidad ya que la educación se vuelve herramienta preventiva. Se enseña ciudadanía digital, el respeto en redes y corresponsabilidad social en el uso de tecnologías, cumpliendo el ODS 4 con visión inclusiva y transformadora.

En cuanto al ODS 5: Igualdad de Género: reconociendo que la igualdad real depende también de garantizar la seguridad y libertad de las mujeres en entornos tecnológicos, donde hoy se reproduce la violencia estructural.

El ODS 9. Industria, Innovación e Infraestructura, este ODS se materializa al introducir el concepto de “responsabilidad digital compartida”: la infraestructura tecnológica no es neutra, y debe proteger derechos humanos. La ley convierte la innovación digital en herramienta de seguridad, no de vulneración.

Y finalmente, el ODS 16: Paz, Justicia e Instituciones Sólidas: mediante el proyecto se consolida instituciones sólidas en el ámbito digital, asegurando el derecho a la justicia y creando mecanismos transparentes de protección, esenciales para la paz y la estabilidad democrática.

Con base a todos los argumentos antes expuestos, se somete al conocimiento y consideración de esta Asamblea Legislativa como un paso fundamental, en el que Costa Rica, como Estado Parte de la Convención de Belém do Pará y de la CEDAW, asume su obligación de prevenir, sancionar y erradicar toda forma de violencia contra las mujeres, incluyendo aquella perpetrada mediante el uso de TIC.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

Expediente N.°25.322

Proyecto de Ley

LEY PARA PREVENIR, ATENDER, PROTEGER, INVESTIGAR, SANCIONAR Y ERRADICAR LA VIOLENCIA DIGITAL CONTRA LAS MUJERES POR RAZONES DE GÉNERO; REFORMA DE LOS ARTÍCULOS 3 y 9 BIS DE LA LEY N.°10235; LOS ARTÍCULOS 7 Y 20 DE LA LEY N.°8968; Y LOS ARTÍCULOS 152, 196, 196 BIS, 196 TER, 196 QUATER Y 196 QUINQUIES DE LA LEY N.°4573

CAPÍTULO I - DISPOSICIONES GENERALES

Artículo 1. Objeto.

Esta Ley tiene por objeto prevenir, atender, proteger, investigar, sancionar y erradicar la violencia digital y mediada por tecnologías informáticas contra las mujeres por razones de género, en los ámbitos público y privado.

Artículo 2. Definición.

Se entiende por violencia digital contra las mujeres por razones de género cualquier acción, conducta, omisión o tolerancia cometida, instigada o agravada mediante el uso de tecnologías en cualquier ámbito de su vida, que cause daño físico, psicológico, sexual, económico o simbólico a una mujer, incluyendo niñas y adolescentes.

Violencia digital de género: Toda acción, omisión o conjunto de conductas realizadas mediante tecnologías de información y comunicación (TIC), que por razones de género cause a una mujer daño físico, psicológico, sexual, económico

o simbólico, o menoscabe sus derechos fundamentales, incluida su dignidad, privacidad, honra, libertad de expresión, participación social, educativa o laboral.

Artículo 3. Principios rectores.

La aplicación de esta Ley se regirá por los principios de igualdad y no discriminación, debida diligencia, dignidad humana, protección integral, progresividad, proporcionalidad, centralidad de las víctimas, no revictimización, gobernanza digital, transparencia y participación interinstitucional.

Igualdad y no discriminación: todas las actuaciones deben respetar la igualdad sustantiva y eliminar sesgos de género.

Debida diligencia reforzada: el Estado debe prevenir, investigar, sancionar y reparar con especial prontitud e idoneidad en entornos digitales.

Interés superior de niñas y adolescentes: prioridad absoluta en medidas, confidencialidad y protección.

Celeridad y precaución: medidas urgentes (24–48 h) cuando exista riesgo de daño o revictimización, aun con evidencia preliminar.

Proporcionalidad y mínima injerencia: retiro/bloqueo/desindexación deben ser específicos y justificados, sin afectar indebidamente otros derechos.

No revictimización y confidencialidad: evitar exposición innecesaria y trato indigno en todas las fases.

Preservación y cadena de custodia digital: toda intervención debe asegurar integridad, autenticidad y trazabilidad de la evidencia.

Transparencia y rendición de cuentas: instituciones y plataformas deben informar plazos, decisiones, recursos y resultados.

Coordinación interinstitucional e internacional: articulación efectiva entre órganos nacionales y cooperación con otros Estados/proveedores.

Artículo 4. Ámbito de aplicación

Se entenderá que la violencia digital contra las mujeres por razones de género es aquella que:

a) Que tenga lugar dentro de cualquier relación interpersonal, incluyendo las relaciones familiares, sexoafectivas, de pareja o expareja, independientemente de que la persona agresora haya o no compartido el mismo domicilio que la mujer.
b) Que tenga lugar en la comunidad y sea perpetrada por cualquier persona.
c) Que sea perpetrada, tolerada, con complicidad o anuencia del Estado o sus agentes, ya sea por la ausencia de políticas de protección y prevención, por inacción ante denuncias de violencia contra las mujeres por razones de género en entornos virtuales, por la adopción de políticas que perpetúen la discriminación y violencia contra las mujeres basada en género en el acceso o uso de tecnologías, o a través de la vigilancia digital sin garantías legales.

Artículo 5. Definiciones

a) Sesgo o prejuicio algorítmico: Situación en la que un sistema de inteligencia artificial produce predicciones o decisiones que generan un trato injusto o desfavorable hacia una persona o grupo de personas, derivado de errores sistemáticos en su diseño o entrenamiento.

b) Proveedor de servicios: Cualquier entidad pública o privada que:
i) Ofrezca a las personas usuarias en el país la posibilidad de comunicarse mediante tecnologías de información y comunicación;
ii) Procese o almacene datos electrónicos en nombre de un servicio de comunicaciones o de sus usuarias o usuarios; o
iii) Diseñe, fabrique o comercialice productos tecnológicos que permitan la captura, almacenamiento, procesamiento o transferencia de datos electrónicos o personales.

c) Moderación de contenidos: Actividades realizadas por los proveedores de servicios, automatizadas o no, destinadas a detectar, identificar, evaluar y actuar respecto de contenidos ilícitos o información contraria a sus términos y condiciones.

d) Intermediarios de internet: Entidades que facilitan la conexión, transmisión y distribución de contenidos entre personas usuarias, tales como motores de búsqueda, plataformas de redes sociales, servicios de mensajería, alojamiento web, plataformas de comercio electrónico y otros equivalentes.

e) Desinformación o difusión de contenidos falsos: Información difundida de manera deliberada e intencionada, a sabiendas de su falsedad, con el fin de generar perjuicio, confusión o manipulación.

f) Entornos o espacios digitales: Espacios virtuales donde se genera, intercambia o consume información, incluyendo plataformas, redes sociales, servicios digitales e infraestructura tecnológica que habilita la interacción.

g) Brecha digital de género: Diferencias entre mujeres y hombres en el acceso, uso, habilidades, oportunidades e impacto de las tecnologías de información y comunicación, influenciadas por estereotipos de género y desigualdades estructurales.

h) Carácter íntimo sexual: Dimensión de la vida privada y de la sexualidad de una persona que involucra autonomía, consentimiento, dignidad y privacidad, y que no guarda relación con asuntos de interés público.

i) Desindexación: Remoción de referencias a contenidos específicos en los resultados de motores de búsqueda, sin perjuicio de su preservación probatoria ordenada por autoridad competente.

j) Retiro o bloqueo de contenido: Inaccesibilidad total o parcial de contenido para el público general o para zonas geográficas específicas, ordenada por autoridad competente y ejecutada por plataformas o proveedores, con preservación probatoria garantizada.

k) Preservación de evidencia digital: Conservación temporal de copias íntegras de contenidos, metadatos, registros, bitácoras y demás elementos necesarios para investigación, con sellado temporal e integridad asegurada.

l) Cadena de custodia digital: Procedimientos técnicos y legales que aseguran autenticidad, integridad, trazabilidad y almacenamiento seguro de evidencia digital desde su obtención hasta su valoración en el proceso judicial.

m) Consentimiento: Manifestación de voluntad libre, informada, específica, inequívoca, verificable y revocable en cualquier momento. El silencio, la inacción o la coacción no constituyen consentimiento.

n) Datos personales y datos sensibles: Aquellos definidos por la Ley N.° 8968. Son sensibles, entre otros, los relativos a salud, vida sexual, biométricos, origen étnico, creencias y geolocalización precisa.

o) Proveedor de servicios digitales: Persona física o jurídica que ofrece, intermedia, hospeda, distribuye, recomienda, clasifica o monetiza contenidos o comunicaciones en línea, incluyendo redes sociales, mensajería, plataformas de video, almacenamiento en nube y motores de búsqueda.

p) Medidas de protección digital: Resoluciones judiciales o administrativas destinadas a cesar el daño y evitar su repetición, que pueden incluir retiro, bloqueo, desindexación, suspensión de monetización, prohibición de contacto digital, restricción de cuentas falsas y medidas de efecto equivalente.

q) Restricciones de proximidad digital: Órdenes que prohíben a una persona determinada contactar, mencionar, etiquetar, enviar mensajes directos o crear cuentas para comunicarse con la víctima por cualquier medio digital.

r) Reparación integral: Medidas destinadas a restituir derechos y atender las consecuencias del daño, que pueden incluir retiro y desindexación de contenidos, disculpas públicas, atención psicológica, medidas de no repetición, capacitación de la persona agresora y compensación económica cuando corresponda.

CAPÍTULO II - DERECHOS DE LAS MUJERES

Artículo 6. Derecho a una vida libre de violencia digital.

Toda mujer tiene derecho a vivir una vida libre de violencia en entornos digitales, garantizándose su seguridad, privacidad, libertad de expresión, participación política y acceso a la justicia.

Artículo 7. Manifestaciones de la violencia digital contra las mujeres por razones de género.

Se consideran manifestaciones de violencia digital contra las mujeres, por razones de género, las siguientes conductas, sin perjuicio de otras que afecten sus derechos fundamentales, su dignidad o su seguridad:

a) Acoso, hostigamiento o persecución digital, mediante el envío reiterado de mensajes, publicaciones, comentarios o imágenes con contenido intimidatorio, degradante, amenazante o sexual no consentido, a través de redes sociales, correos electrónicos, plataformas digitales, mensajería instantánea u otros medios tecnológicos.
b) Difusión, publicación o reenvío de imágenes, videos, audios o cualquier material de contenido íntimo o sexual sin consentimiento de la mujer que aparece en ellos, incluyendo aquellos generados o manipulados mediante inteligencia artificial, “deepfakes” u otras herramientas tecnológicas.
c) Suplantación de identidad o creación de perfiles falsos, con el fin de manipular, engañar, difamar, dañar la reputación, obtener beneficios o ejercer control, acoso o intimidación hacia una mujer.
d) Amenazas, coacción o chantaje digital, mediante la utilización de información personal, imágenes, datos íntimos o comunicaciones privadas para obtener favores sexuales, económicos, políticos o de cualquier otra índole.
e) Acceso, sustracción, manipulación o divulgación no autorizada de información personal, comunicaciones privadas o datos digitales de una

mujer, incluyendo geolocalización, contraseñas, contenido almacenado o datos biométricos.

f) Creación o difusión de discursos de odio, mensajes misóginos o discriminatorios en entornos digitales, que tengan por objeto menoscabar la dignidad, reputación o integridad emocional de las mujeres, especialmente de aquellas con participación pública o política.
g) Distribución de desinformación o contenidos falsos, que busquen desacreditar, ridiculizar, silenciar o deslegitimar la voz pública de las mujeres o fomentar estereotipos y violencias estructurales.
h) Utilización de tecnologías de seguimiento, espionaje o monitoreo digital sin consentimiento, incluyendo software espía, dispositivos de rastreo, grabaciones, vigilancia no autorizada o control remoto de dispositivos electrónicos.
i) Ataques coordinados o campañas digitales de hostigamiento, orientadas a saturar redes, páginas o cuentas de mujeres con mensajes violentos o difamatorios, con el fin de forzarlas al silencio o a la autocensura.
j) Cualquier otra conducta cometida mediante el uso de tecnologías de la información o comunicación que atente contra el derecho de las mujeres a vivir libres de violencia, discriminación y acoso en espacios digitales o mediáticos.
k) La divulgación de contenido íntimo: Imágenes, audios o videos de carácter sexual, erótico, o que muestren partes del cuerpo usualmente cubiertas, y que fueron obtenidos o compartidos en un contexto de privacidad o confianza.
l) La difusión no consentida de contenido íntimo: Publicar, compartir, reenviar, poner a disposición o amenazar con difundir contenido íntimo de una mujer sin su consentimiento expreso, cualquiera sea el medio o plataforma, haya sido o no la mujer quien produjo el material.
m) El deepfake sexual o manipulación sexual digital: Cualquier imagen, audio o video generado o alterado mediante técnicas digitales, incluida la inteligencia artificial, que simule o atribuya a una mujer actos, expresiones o rasgos de

carácter sexual sin su consentimiento, con fines de humillación, extorsión, lucro o denigración.

n) La sextorsión: Amenazar con difundir contenido íntimo, datos personales o información dañina de una mujer para obtener actos de naturaleza sexual, dinero, favores, decisiones o cualquier ventaja indebida.

o) El ciberacoso u hostigamiento digital: Conducta reiterada a través de medios digitales (mensajes, publicaciones, comentarios, etiquetas, reacciones, llamadas, correos, foros, videojuegos u otros) que tenga por objeto o efecto intimidar, degradar, avergonzar, amenazar, perturbar la tranquilidad o aislar a una mujer.

p) El acoso en masa o “brigading”: Ataques coordinados o simultáneos por múltiples cuentas, grupos o usuarios hacia una mujer, que generen saturación de mensajes, denuncias falsas, reportes coordinados o tendencias hostiles.

q) Bots, “troll farms” y “astroturfing”:

   a) Bot: cuenta automatizada o parcialmente automatizada que interactúa simulando personas, con el fin de amplificar o dirigir ataques.

   b) Troll farm: organización o grupo estructurado que opera múltiples cuentas para hostigar o manipular conversaciones.

   c) Astroturfing: simulación de apoyo u oposición masiva con cuentas coordinadas o falsas, para aparentar legitimidad o consenso e incidir en la reputación de una mujer.

r) El doxing (exposición de datos): Obtención, compilación y divulgación no autorizada de datos personales o sensibles de una mujer (por ejemplo: dirección, números de identificación, datos biométricos, ubicación, datos de hijos o familiares, contraseñas o información de salud) con potencial de riesgo para su seguridad, integridad o privacidad.

s) La suplantación de identidad: Creación, uso o control de cuentas, sitios, perfiles o medios que simulen ser una mujer específica, con finalidad de engaño, daño reputacional, fraude, lucro, acoso o captación de información privada.

t) La intrusión en dispositivos, cuentas o redes: Acceso no autorizado a cualquier dispositivo, aplicación, cuenta, almacenamiento en la nube, correo o comunicación digital de una mujer, incluyendo la instalación de software espía, vigilantes o de rastreo (conocidos como “stalkerware”), o la interceptación ilícita de comunicaciones.
u) La vigilancia y geolocalización abusiva: Uso no autorizado o desproporcionado de funciones de ubicación, seguimiento o monitoreo, que permita conocer o inferir rutinas, recorridos, domicilios o contactos de una mujer.
v) La violencia simbólica digital: Producción, difusión o reproducción de estereotipos, mensajes, imágenes, memes o narrativas que desvaloricen a las mujeres por su condición de género y que, por su masividad o repetición, generen entornos hostiles, de humillación o exclusión.
w) La OSINT abusiva (investigación abierta maliciosa): Búsqueda y correlación de información pública o semipública sobre una mujer, con el fin de exponerla a riesgos, daño reputacional o extorsión.
x) Violencia política digital contra las mujeres: Uso de plataformas, redes, grupos digitales, perfiles institucionales o cuentas anónimas para atacar, humillar, desacreditar, difamar, sexualizar, amenazar o deslegitimar a mujeres que ejercen funciones públicas, liderazgo social, participación ciudadana o actividad política, con el fin de impedir, obstaculizar o anular el ejercicio de sus derechos.
y) Cualquier otra conducta realizada mediante tecnologías digitales que, por razones de género, cause daño físico, psicológico, sexual, económico, político, reputacional o simbólico a una mujer.

Artículo 8. 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.

CAPÍTULO III - DEBERES DEL ESTADO

Artículo 9. Medidas de protección y atención.

El Instituto Nacional de las Mujeres (INAMU), como ente rector en materia de igualdad y derechos de las mujeres, en coordinación con el Ministerio de Justicia y Paz, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Poder Judicial, el Ministerio Público y la Defensoría de los Habitantes, y representantes de proveedores de servicios digitales, deberá garantizar la atención integral, accesible, inmediata y con perspectiva de género a las víctimas de violencia digital o mediada por tecnologías.

Para estos efectos, deberán adoptarse las siguientes acciones:

a) Establecer protocolos especializados de atención y derivación para mujeres víctimas de violencia digital, con mecanismos ágiles de atención de denuncias, protección de evidencia digital y acompañamiento jurídico, psicológico y social.
b) Crear y fortalecer servicios de orientación, asesoría y acompañamiento en línea y presenciales, accesibles desde todo el territorio nacional, garantizando confidencialidad y atención libre de estigmas.
c) Asegurar la capacitación permanente del personal de los servicios públicos en materia de violencia digital, con énfasis en las particularidades de género, interseccionalidad, privacidad digital y derechos humanos.
d) Impulsar campañas nacionales de educación y sensibilización digital con enfoque de género, dirigidas a niñas, adolescentes y mujeres adultas, para la prevención del acoso, la sextorsión, la manipulación y la violencia simbólica en entornos digitales. Asimismo a toda la población, para promover la alfabetización digital en todos los niveles del currículo educativo, garantizando un acceso equitativo y responsable a la tecnología, fomentando la participación activa y segura de las mujeres, niñas y adolescentes en el entorno digital.

Artículo 10. Medidas cautelares y de protección de urgencia.

Las autoridades judiciales competentes, incluyendo los Juzgados de Violencia Doméstica, el Ministerio Público, de oficio o a solicitud de la víctima o del INAMU, podrán dictar medidas cautelares o de protección inmediata cuando existan indicios razonables de que una mujer está siendo víctima de violencia digital.

Entre las medidas podrán ordenarse:

a) Instruir al proveedor de servicios digitales La eliminación inmediata o bloqueo temporal de material digital o contenido que constituya violencia, garantizando la preservación de la evidencia para fines judiciales.
b) La prohibición de contacto digital o físico de la presunta persona agresora con la víctima por cualquier medio tecnológico o red social.
c) Instruir al proveedor de servicios digitales La suspensión del acceso a cuentas, plataformas o dispositivos electrónicos utilizados para agredir o difundir material ilícito.
d) Cualquier otra medida necesaria para evitar la revictimización o la continuación del daño, conforme a los principios de legalidad, proporcionalidad y urgencia.

El Poder Judicial desarrollará un protocolo digital de ejecución rápida de estas medidas en coordinación con los proveedores de servicios tecnológicos y las autoridades de ciberseguridad y el Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT).

Artículo 11. Sanción por incumplimiento de medidas cautelares o de protección de urgencia.

El incumplimiento total o parcial de las medidas cautelares o de protección dictadas conforme al artículo anterior constituirá delito de desobediencia a la autoridad, conforme al artículo 314 del Código Penal, sin perjuicio de las sanciones adicionales

que pudieren corresponder por los hechos de violencia digital que dieron origen a la medida.

Cuando la persona agresora incumpla una medida de protección dictada a favor de una mujer víctima de violencia digital, el Juzgado competente comunicará de inmediato los hechos al Ministerio Público, a efectos de la apertura de la causa penal correspondiente. En estos casos, se presumirá la intencionalidad de la conducta cuando existan actos de reiteración, contacto digital o difusión posterior del material objeto de la medida.

Sin perjuicio de la responsabilidad penal que corresponda, el incumplimiento de las medidas acarreará la imposición de sanciones administrativas o disciplinarias cuando la persona agresora sea funcionaria pública, de conformidad con la normativa vigente.

Artículo 12. Asistencia jurídica y acompañamiento integral.

La Defensa Publica, en coordinación con el INAMU y el Ministerio de Justicia y Paz, garantizará a las víctimas de violencia digital asistencia jurídica gratuita, especializada y con enfoque de género.

El INAMU deberá mantener un registro de los casos atendidos y promover la articulación con organizaciones de la sociedad civil y universidades públicas para brindar acompañamiento psicológico, social y jurídico a las víctimas.

Artículo 13. Prevención y atención de la violencia digital política.

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 deberán adoptar políticas, protocolos y mecanismos de coordinación institucional para prevenir, atender y dar acompañamiento integral a las mujeres que enfrenten violencia digital por razones de género en el ejercicio de cargos públicos, precandidaturas, candidaturas o participación política.

Estas acciones incluirán:

a) Mecanismos accesibles de denuncia, orientación y protección inmediata, con articulación directa hacia las autoridades judiciales y electorales competentes para la emisión de medidas cautelares y órdenes de retiro de contenido.

b) Sistemas de análisis y monitoreo no punitivo de riesgos, con fines preventivos y estadísticos, orientados a identificar patrones de ataques digitales, discursos de odio, campañas de desinformación o dinámicas que puedan afectar el ejercicio de los derechos políticos de las mujeres, respetando la privacidad y la normativa de protección de datos.

c) Protocolos de enlace y cooperación con plataformas digitales, encaminados a facilitar el reporte ágil de contenidos presuntamente ilícitos, promover la preservación de evidencia y asegurar la comunicación oportuna con las autoridades judiciales encargadas de ordenar, cuando corresponda, el retiro, bloqueo o desindexación de contenidos.

d) Capacitación obligatoria para partidos políticos, autoridades electorales y representantes institucionales sobre prevención, identificación, acompañamiento y manejo adecuado de la violencia digital de género en procesos políticos o electorales.

e) Rutas de atención integral, coordinadas con INAMU, Defensoría, Tribunal Supremo de Elecciones (TSE) y Poder Judicial, para garantizar apoyo psicológico, legal, social y tecnológico a las mujeres afectadas.

Artículo 14. Unidad especializada en violencia digital y cibercrimen (UEVDC)

Crease la Unidad especializada en violencia digital y cibercrimen conformada por un representante en propiedad y un suplente de:

a) La oficina de atención y protección de la víctima del Ministerio Público
b) La Unidad de cibercrimen del Ministerio Público
c) La Sección de Delitos Informáticos del Organismo de Investigación Judicial

d) El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)
e) El Instituto de la Mujer INAMU

Artículo 15. Funciones de la Unidad especializada en violencia digital y cibercrimen (UEVDC)

Las funciones de la UEVDC serán:

a) Investigar las denuncias interpuestas en las distintas dependencias
b) Coordinar las acciones interinstitucionales para preservar la evidencia digital, hacer el seguimiento de los casos y proceder con las medidas cautelares y de protección de las víctimas.
c) Asegurar la cooperación internacional en casos transnacionales, conforme a los tratados y convenios suscritos por la República.
d) Solicitar el debido presupuesto equitativo de las representaciones ante sus debidas instancias.

CAPÍTULO IV - RESPONSABILIDADADES Y REGIMEN SANCIONATORIO POR VIOLENCIA DIGITAL HACIA LAS MUJERES EN RAZÓN DE GÉNERO

Artículo 16. Obligaciones de los proveedores de servicios digitales.

Los proveedores de servicios digitales deberán implementar mecanismos de denuncia accesibles, rápidos y eficientes, la moderación de contenidos con perspectiva de género, notificación a la Unidad especializada en violencia digital y cibercrimen_ante sospecha de violencia digital, así como contar con políticas de transparencia sobre uso de datos y algoritmos.

Artículo 17. Régimen sancionatorio para proveedores de servicios digitales.

Los proveedores de servicios digitales, nacionales o internacionales, que operen, presten servicios o mantengan personas usuarias en el territorio nacional estarán sujetos a responsabilidad administrativa y civil por el incumplimiento de las obligaciones establecidas en esta Ley.

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en coordinación con el Instituto Nacional de las Mujeres (INAMU) y la Defensoría de los Habitantes, ejercerá la potestad sancionadora administrativa, respetando el debido proceso y garantizando la proporcionalidad de las medidas. Podrá imponer una o varias de las siguientes sanciones:

a) Advertencia formal: Comunicación escrita dirigida al proveedor infractor, mediante resolución motivada, señalando la conducta incumplida y ordenando la adopción de medidas correctivas dentro de un plazo razonable.

b) Multas administrativas: Multas proporcionales a la gravedad de la infracción, al número de personas afectadas, al nivel de cooperación del proveedor y a su capacidad económica. Las multas oscilarán entre diez (10) y doscientos (200) salarios base.

Los recursos provenientes de estas multas se transferirán al Instituto Nacional de las Mujeres (INAMU) y se destinarán exclusivamente al financiamiento de acciones de prevención, atención, alfabetización digital y apoyo a víctimas de violencia digital, conforme a los lineamientos del PLANOVI.

c) Órdenes de adopción de medidas correctivas: El proveedor sancionado deberá implementar, bajo su costo, medidas técnicas y operativas que garanticen la prevención y no repetición de la conducta infractora, tales como:

a. fortalecimiento de mecanismos de denuncia;
b. mejoras en tiempos de respuesta;
c. ajustes en procesos de verificación o moderación;

d. adecuaciones algorítmicas cuando sean necesarias y proporcionadas;
e. mejoras de seguridad para usuarias afectadas;
f. capacitación de su personal en violencia digital de género.

d) Auditorías externas obligatorias, la autoridad competente podrá ordenar auditorías independientes, técnicas y razonables sobre los procesos de reporte, atención y mitigación de violencia digital, a cargo del proveedor, como medida para asegurar el cumplimiento normativo.

e) Informes de transparencia: Los proveedores sancionados deberán presentar informes anuales de transparencia que incluyan:

a. número de denuncias recibidas,
b. tipo de violencia digital reportada,
c. tiempos de respuesta,
d. medidas adoptadas,
e. cooperación con autoridades nacionales.
f. Los informes serán públicos, accesibles y deberán contener datos desagregados por género.

f) Suspensión de servicios comerciales no esenciales; en caso de incumplimiento grave y reiterado, el MICITT podrá ordenar la suspensión temporal de funcionalidades comerciales no esenciales (como monetización, publicidad dirigida u otros servicios accesorios), siempre que ello no afecte el derecho de las personas usuarias a la comunicación, libertad de expresión o acceso a la información. Las sanciones establecidas en este artículo se aplicarán sin perjuicio de la responsabilidad civil o penal que corresponda a las personas físicas o jurídicas involucradas.

Las sanciones previstas en este artículo se aplicarán sin perjuicio de la responsabilidad civil o penal que corresponda a las personas físicas o jurídicas involucradas. El INAMU rendirá cuentas anualmente sobre la ejecución de los recursos provenientes de las multas y medidas correctivas.

Artículo 18. Responsabilidad de las personas funcionarias públicas.

Las personas funcionarias públicas, en el ejercicio de sus competencias, estarán obligadas a actuar con debida diligencia reforzada para prevenir, atender, proteger, investigar, sancionar y erradicar cualquier manifestación de violencia digital o mediada por tecnologías contra las mujeres por razones de género.

Constituye falta grave el incumplimiento de las obligaciones funcionales que tenga por efecto la omisión, negligencia, demora injustificada o inacción ante hechos denunciados o conocidos de violencia digital, especialmente cuando la persona funcionaria:

a) Tenga conocimiento de la posible comisión de actos de violencia digital o mediada por tecnologías contra mujeres y, estando legalmente obligada, no adopte medidas inmediatas de protección, atención o denuncia ante las autoridades competentes.
b) Obstaculice, minimice, desestime o revictimice a la denunciante, o emita valoraciones basadas en estereotipos de género, prejuicios o juicios morales que afecten su derecho de acceso a la justicia y a la protección efectiva.
c) Difunda, manipule, sustraiga o comparta información sensible, privada o íntima de las mujeres víctimas, en violación de los deberes de confidencialidad y protección de datos personales establecidos en la Ley N.º 8968.
d) Ejecute, instigue o participe directa o indirectamente en actos de violencia digital, acoso, difusión no consentida de material íntimo, o cualquier otra conducta que vulnere derechos de mujeres bajo su jerarquía, tutela o relación institucional.

El incumplimiento de estas obligaciones dará lugar a responsabilidad administrativa, civil o penal, según corresponda, conforme a la legislación nacional vigente.

Las sanciones podrán incluir suspensión, destitución, inhabilitación para el ejercicio de cargos públicos y las consecuencias penales que determinen los tribunales de justicia.

El INAMU, como ente rector, deberá coordinar con todas las instituciones públicas el desarrollo de protocolos de actuación institucional y módulos de formación obligatoria en perspectiva de género digital, con el fin de prevenir la violencia institucional y garantizar el cumplimiento de los deberes funcionales establecidos en esta Ley.

CAPÍTULO V PROCESOS JUDICIALES Y GARANTÍAS PROCESALES

Artículo 19. Principios especiales aplicables a los procesos de violencia digital.

Sin perjuicio de las garantías constitucionales y procesales ya vigentes, los procesos relacionados con violencia digital contra las mujeres se regirán por los siguientes principios específicos:

a) Debida diligencia digital reforzada: Las autoridades deberán actuar con especial celeridad dada la volatilidad, velocidad de propagación y facilidad de alteración o eliminación del contenido digital.

b) Eficacia probatoria digital: La obtención, recolección, preservación, cadena de custodia y análisis de evidencia digital deberán realizarse conforme a protocolos técnicos actualizados y estándares internacionales.

c) Protección reforzada de datos personales y de identidad digital: Las actuaciones deberán garantizar la confidencialidad de la información sensible, íntima o privada de las mujeres afectadas.

d) No revictimización digital: Se evitará la reproducción innecesaria de contenido íntimo, humillante o degradante en los expedientes, audiencias o actuaciones judiciales.

e) Enfoque de género e interseccionalidad**:** La valoración judicial de la prueba incorporará la comprensión de estereotipos digitales, violencia simbólica, amenazas en línea y dinámicas específicas de agresiones mediante tecnologías.

Artículo 20. Derechos especiales de las mujeres en procesos por violencia digital.

Además de los derechos procesales generales, toda mujer víctima tendrá derecho a:

a) Asistencia jurídica y psicosocial especializada, con conocimiento en violencia digital.
b) Participación informada sobre cada etapa del proceso, incluyendo medidas cautelares digitales.
c) Protección de su identidad digital, evitando exposiciones indebidas.
d) Medidas de seguridad digital inmediatas, según criterio del juzgado competente.
e) Atención diferenciada para niñas, adolescentes, mujeres con discapacidad o en situación de vulnerabilidad.

Artículo 21. Investigación y evidencia digital.

El Ministerio Público y el Organismo de Investigación Judicial (OIJ) deberán:

Aplicar protocolos técnicos de evidencia digital, garantizando autenticidad, integridad y preservación.
b) Actuar con celeridad reforzada para asegurar la recolección oportuna del contenido.
c) Incorporar capacitación especializada continua en violencia digital y perspectiva de género.
d) Establecer canales oficiales de cooperación con proveedores de servicios

digitales, exclusivamente para preservación de evidencia, identificación de cuentas y cumplimiento de órdenes judiciales.
e) Activar cooperación internacional cuando existan elementos ubicados fuera del territorio nacional.

Artículo 22. Justicia restaurativa y reparación integral.

Podrán promoverse procesos de justicia restaurativa en casos de violencia digital cuando:
a) La naturaleza de los hechos lo permita;
b) Exista consentimiento libre, previo e informado de la víctima;
c) No exista relación de poder, dependencia o subordinación entre la víctima y la persona agresora; y
d) No se trate de conductas que involucren menores de edad, sextorsión, deepfakes sexuales o difusión no consentida de contenido íntimo con daño grave.
Los procesos de justicia restaurativa:
Serán dirigidos y supervisados exclusivamente por el Poder Judicial, conforme a la Ley de Resolución Alterna de Conflictos y su reglamento.
Podrán incluir medidas de reparación simbólica, disculpas voluntarias, compromisos de no repetición y la entrega o eliminación del contenido bajo autorización judicial.
En ningún caso sustituirán medidas cautelares ni limitarán la facultad del juez para ordenar preservación probatoria o retiro de contenido.
El INAMU, el Ministerio de Justicia y Paz y el MICITT podrán desarrollar programas de alfabetización digital, ciudadanía responsable y formación en igualdad de género orientados a la prevención, pero no participarán en los procedimientos de justicia restaurativa.

CAPÍTULO VI - REFORMAS A LEYES VIGENTES

Artículo 23. Reforma a la Ley N.° 10235, “Ley para Prevenir, Atender, Sancionar y Erradicar la Violencia contra las Mujeres en la Política”.

Se adicionan los siguientes artículos:

Artículo 3 bis. Violencia político-digital.
Se reconoce como modalidad de violencia política contra las mujeres aquella que se comete mediante el uso de tecnologías de la información y la comunicación, plataformas digitales o redes sociales, dirigida a afectar, limitar o anular el ejercicio de los derechos políticos, la participación o el desempeño en cargos públicos de las mujeres.

Artículo 9 bis. Medidas digitales urgentes.
Durante procesos electorales, precampañas, campañas o el ejercicio de un cargo público, la autoridad judicial competente podrá ordenar, en un plazo de veinticuatro (24) a cuarenta y ocho (48) horas:
a) la desindexación de contenido;
b) el retiro temporal de publicaciones;
c) el bloqueo geográfico;
d) la preservación probatoria de contenido digital;
e) cualquier otra medida proporcional de protección digital.
La solicitud deberá ser tramitada con debida diligencia reforzada y enfoque de género.

Artículo 24. Reforma a la Ley N.º 8968, “Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales”.
Se adicionan los siguientes artículos:

Artículo 7 bis. Procedimiento abreviado de desindexación y retiro en casos de violencia digital.
Cuando una mujer sea víctima de difusión no consentida de contenido íntimo, deepfakes, suplantación de identidad digital o manipulación sexualizada, podrá solicitar a la autoridad judicial un procedimiento abreviado para:
a) la desindexación del contenido,

b) el retiro temporal de publicaciones,
c) la preservación probatoria digital.
La autoridad judicial deberá resolver en un plazo máximo de cuarenta y ocho (48) horas.

Artículo 20 bis. Coordinación PRODHAB–Poder Judicial.
La Agencia de Protección de Datos de los Habitantes (PRODHAB) establecerá protocolos de cooperación con el Poder Judicial para asegurar:
a) la preservación oportuna de evidencia digital,
b) la atención urgente a solicitudes judiciales,
c) la coordinación con proveedores de servicios digitales para asegurar el cumplimiento de órdenes judiciales.

Artículo 25. Reformas al Código Penal, Ley N.º 4573.

Se adicionan los siguientes artículos:

Artículo 196 bis. Difusión no consentida de contenido íntimo (NCII).
Quien difunda, publique, comparta, revele o ponga a disposición de terceros imágenes, audios o videos de carácter íntimo o sexual, sin consentimiento de la persona que aparece en ellos, será sancionado con pena de prisión de uno (1) a cuatro (4) años.
La pena será de dos (2) a cinco (5) años si:
a) existe fin de lucro;
b) la víctima es menor de edad;
c) se utilizó suplantación de identidad;
d) se ocasionó daño grave a la salud mental o física de la víctima.

Artículo 196 ter. Manipulación digital sexualizada (deepfake sexual).

Quien genere, altere, manipule o difunda imágenes, audios o videos de carácter sexual atribuidos falsamente a una mujer, mediante inteligencia artificial u otras técnicas digitales, será sancionado con pena de prisión de dos (2) a seis (6) años.

Artículo 196 quater. Sextorsión digital.
Quien, mediante amenaza de revelar contenido íntimo, datos personales o información degradante, obligue a una mujer a realizar actos sexuales, entregar dinero o favores, será sancionado con prisión de tres (3) a siete (7) años.
La pena será de cuatro (4) a diez (10) años si:
a) la víctima es menor de edad;
b) la amenaza se realiza a través de medios masivos, cuentas coordinadas o campañas digitales.

Artículo 196 quinquies. Doxing agravado.
Quien divulgue, comparta o publique datos personales o sensibles de una mujer, con potencial de causar daño o riesgo, será sancionado con pena de prisión de uno (1) a tres (3) años.
La pena será de dos (2) a cuatro (4) años si:
a) se produce acoso digital o físico,
b) se genera daño económico o laboral,
c) se pone en riesgo a menores bajo su cuidado.

Artículo 152 bis. 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 (6) meses a dos (2) años.
La pena será de uno (1) a tres (3) 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.

CAPÍTULO VII - EDUCACIÓN

Artículo 26. Educación y campañas.

El INAMU ejecutará campañas anuales de seguridad digital con enfoque de género y denuncia segura en redes.

CAPÍTULO VIII - TRANSITORIOS

Transitorio 1. Reglamentación.

El Poder Ejecutivo reglamentará la presente Ley en un plazo de seis meses a partir de su publicación.

Esta Ley rige a partir de su publicación en el Diario Oficial La Gaceta.

Cynthia Córdoba Serrano **Luz Mary Alpízar Loaiza**

DIPUTADAS

Lista de diputadas y diputados firmantes