

LEY OLIMPIA: MEMORIA HISTÓRICA DE UNA CAUSA QUE INICIARON LAS VÍCTIMAS DE VIOLENCIA DIGITAL.

Desde el año 2013 en México, un grupo de mujeres jóvenes, sobrevivientes de una violencia que no tenía nombre aún, iniciaron juntas una lucha que, para 2019 ya se había extendido por América Latina para visibilizar, reconocer, definir, prevenir, atender, sancionar y erradicar, a través de las leyes, las políticas y de una transformación cultural, lo que ahora conocemos como “violencia digital”.

En 2014 por primera vez redactaron y presentaron como movimiento un conjunto de reformas legislativas únicas en su tipo para la época. Cada párrafo, cada palabra de la propuesta era el reflejo de sus propias historias y las de muchas mujeres más que habían sido violentadas en un espacio que se pensaba que no era real, el ámbito digital. Dicho conjunto de reformas legales, fueron denominadas por los medios de comunicación como “Ley Olimpia” (en honor a Olimpia Coral Melo, fundadora del movimiento). Para el año 2021 miles de mujeres se habían apropiado de esta causa, haciendo realidad la Ley Olimpia en las 33 entidades de México y a nivel federal.

Mientras tanto, desde 2019 en Argentina y 2020 en Ecuador, otras mujeres jóvenes sobrevivientes de violencia digital, también luchaban para que en sus países se aprobara la Ley Olimpia, lográndolo en 2023 y 2021 respectivamente. En 2024 se aprobó en el congreso de Panamá y para 2025 activistas y sobrevivientes de violencia digital en Colombia, Uruguay, República Dominicana, Honduras, Bolivia, Guatemala y otros países de la región, luchan para que la Ley Olimpia llegue a sus países.

Ley Olimpia no es sólo un conjunto de reformas legales, es una causa integral contra la violencia digital de género. Hoy es el nombre también del movimiento feminista latinoamericano nacido en cada territorio donde las víctimas han luchado por la reivindicación de sus historias de vida, que la violencia digital alguna vez destruyó.

Las mujeres que han encarnado este movimiento, son ahora una red Latinoamericana de Defensoras Digitales y a través de la Ley Olimpia no sólo han transformado las leyes, han creado protocolos, impulsado políticas, capacitado instituciones, diseñaron una metodología de atención a víctimas, han impulsado acciones preventivas, han desarrollado tecnología con enfoque feminista... todo para hacer frente a la violencia digital y eliminar sus efectos nocivos. Todo sin el privilegio del poder económico, ni institucional, todo desde el dolor y la digna rabia transformada en amor colectivo, todo siempre poniendo en el centro a las víctimas y sobrevivientes de violencia digital.

Es por eso que esta Ley Modelo retoma el legado de este movimiento vivo en las Américas y se suma a sus voces para decir que “Lo virtual es real”, que “no es porno, ni venganza, es violencia digital”, para denunciar la existencia del “algoritmo patriarcal” y del Imperio Digital que ha concentrado poder de información, tecnológico, económico y político, agravando las brechas de desigualdad entre países y personas; para enfatizar la responsabilidad de los agresores, y luchar por la no deshumanización de las mujeres en los espacios digitales.

Porque una forma justa de revindicar a las mujeres es no borrarlas de la historia. Desde MESECVI y OEA se reconoce el trabajo de cientos de mujeres latinoamericanas que desde muy diversos espacios han luchado contra la violencia digital, que la han estudiado, teorizado, atendido casos y emprendido acciones para prevenirla, incluyendo desde luego al movimiento “Ley Olimpia”, que fijó los primeros aportes para una legislación pionera en materia de violencia digital en las Américas.



“A las víctimas, a las que decenas de veces que nos regresamos con el cuerpo roto y la piel herida cuando íbamos a denunciar y nos dijeron que no había delito que perseguir porque lo virtual no era real. Por las decenas de señalamientos sociales y las decenas de voces que nos juzgaron por nuestro cuerpo desnudo exhibido sin consentimiento en internet. Por las muchas que quisimos morir y sentimos vergüenza de nuestros cuerpos cuando nos enfrentamos en nuestros Países al aparato del Estado y nos dijeron que de esta violencia no podíamos hacer nada. Por ellas, por nosotras, por el camino recorrido para que hoy nuestras voces tengan justicia en una ley modelo que forjamos juntas y que se inspira en la lucha colectiva a la que llamamos la Ley Olimpia”

Defensoras Digitales de América Latina

OBSERVACIONES AL BORRADOR DE LA LEY MODELO INTERAMERICANA PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA DIGITAL CONTRA LAS MUJERES POR RAZONES DE GÉNERO

Artículo / Fragmento	Texto del Documento	Texto sugerido	Observaciones o Argumentación
Artículo 1	Esta ley tiene por objeto la prevención, atención, protección, investigación, sanción, reparación de los daños y erradicación de la violencia digital contra las mujeres por razones de género tanto en el ámbito público como privado, instigada, mediada o con el uso de las tecnologías.	Esta ley tiene por objeto la prevención, atención, protección, investigación, sanción, reparación de los daños y erradicación de la violencia digital contra las mujeres por razones de género tanto en todos los ámbitos de su existencia, que sea cometida, instigada, mediada, agravada total o parcialmente por medio del uso de tecnologías digitales y emergentes.	Nombrar sólo los ámbitos público y privado, pueden no ser suficientemente abarcativo. La ley refiere en particular a la violencia digital que puede ser ejercida sólo a través del uso de tecnologías digitales, no cualquier tipo de tecnología desarrollada con anterioridad, sin embargo, es posible extender su vigencia colocando la palabra “emergentes” para que abarque aquellas tecnologías que aún no se han desarrollado.
Artículo 2	Cualquier acción, conducta u omisión contra las mujeres, basada en su género, que cause muerte, daño o sufrimiento físico, sexual, psicológico, económico o simbólico, en cualquier ámbito de su vida, que sea cometida, instigada o agravada, en parte o en su totalidad, con el uso de las tecnologías.	Cualquier acción, conducta u omisión contra las mujeres, basada en su género, que cause muerte, daño o sufrimiento físico, sexual, psicológico, económico, patrimonial o simbólico, en cualquier ámbito de su vida, que sea cometida, instigada o agravada, en parte o en su totalidad, con el uso de las tecnologías digitales y emergentes.	La ley refiere en particular a la violencia digital que puede ser ejercida sólo a través del uso de tecnologías digitales, no cualquier tipo de tecnología desarrollada con anterioridad, sin embargo, es posible extender su vigencia colocando la palabra “emergentes” para que abarque aquellas tecnologías que aún no se han desarrollado.
Art. 3. 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 el agresor 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 aquiescencia 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	Se entenderá que la violencia digital contra las mujeres por razones de género es una modalidad de violencia que puede ser cometida, instigada, agravada, tolerada o fomentada en los ámbitos público, privado o íntimo, de manera interseccional con cualquiera de las siguientes modalidades (de manera enunciativa, no limitativa): <ul style="list-style-type: none">• Familiar o Interpersonal -• Escolar -• Laboral y docente-• Comunitario -• Político -• Mediático -• Gubernamental o institucional (Estado) -• Empresarial, corporativo, algorítmico – por los proveedores de Internet, de plataformas digitales y de streaming, sitios web, redes sociales, buscadores,	Con esta redacción quedan especificados los ámbitos público y privado, que ya se mencionaban en la redacción original, pero se agrega el ámbito íntimo (pensando en las violaciones a la intimidad), además de que se especifican las modalidades de violencia que constituyen también ámbitos de ocurrencia de la violencia digital. Se sugiere incluir una explicación para comprender cada uno con base en bibliografía feminista y legislaciones ya vigentes en el continente (como la Ley de acceso de las mujeres a una vida libre de violencia de México). Sabido que el último inciso no es nombrado en documentos previos, se agrega una explicación sugerida (sujeta a ser perfeccionada), por la relevancia de enfatizar la gran responsabilidad de las empresas

	el acceso o uso de tecnologías, o a través de la vigilancia digital sin garantías legales.	aplicaciones, las productoras de contenidos digitales o el conjunto de ellos, ya sea que redunde o no en beneficios económicos para ellos, por los mecanismos a su alcance, incluyendo la programación algorítmica.	y los corporativos de Big Tech en la problemática y la enorme necesidad, de que adquieran responsabilidades y se limite el poder económico, político, tecnológico y de información que han acumulado en la actualidad.
Art. 6. Inciso b	Protección de su integridad física, psíquica y emocional frente a cualquier forma de violencia digital por razones de género;	Protección de su integridad física, psíquica, emocional, sexual frente a cualquier forma de violencia digital por razones de género;	Únicamente se agrega la protección explícita a la integridad sexual.
Art. 6. Inciso c	Libertad y seguridad personal, incluyendo la libertad de participar en espacios digitales sin temor a represalias	Libertad y seguridad personal, incluyendo la libertad de participar en espacios digitales sin temor a represalias o ataques .	Se agrega la palabra “ataques”, suponiendo que represalias vendrían del Estado y los ataques de personas o grupos civiles.
Artículo 7. Manifestaciones de la violencia digital contra las mujeres por razones de género.	b. “Manipular, engañar o explotar a una mujer para que envíe imágenes...”		El verbo “manipular” es demasiado amplio y subjetivo. Puede prestarse a interpretaciones ambiguas. Se sugiere precisar los alcances de la manipulación, o al menos requerir algún elemento probatorio adicional para evitar abusos del marco legal. Algunos aportes para sumar a la elaboración del texto se pueden encontrar en las notas adicionales a este documento.
Artículo 9 Medidas de política pública de prevención	Serán competentes para la aplicación de estas medidas el Mecanismo Nacional de las Mujeres, como ente rector, en coordinación con los órganos reguladores de Tecnologías de la Información y las Comunicaciones, Ciencia, control digital, Estadística, Educación e Industria y Comercio, órganos electorales y otras instituciones a las que la ley le atribuya competencia. Estos órganos deberán adoptar medidas integrales para prevenir la violencia digital contra las mujeres por razones de género, abordar sus causas estructurales y frenar amenazas y violaciones de derechos humanos, actuando con debida diligencia reforzada. Lo que incluye, entre otras: a. Establecer una mesa interinstitucional y multiactor, regulada mediante decreto, que incluya la participación del	El Estado, a través de sus órganos de gobierno competentes, debe asegurar la adopción de medidas integrales para prevenir la violencia digital contra las mujeres por razones de género, abordar sus causas estructurales y frenar amenazas y violaciones de derechos humanos, actuando con debida diligencia reforzada. Lo que incluye, entre otras: a. Establecer una mesa interinstitucional y multidisciplinaria, que incluya la participación del gobierno, del sector privado, sociedad civil (academia, organizaciones, defensoras de derechos humanos, víctimas de violencia digital) y comunidad técnica. Esta mesa se reunirá de manera periódica para coordinar acciones y desarrollar estrategias conjuntas de gobernanza digital abierta, inclusiva, transparente y con perspectiva de género;	Se debe considerar que en muchos países no existe un Mecanismo Nacional de las Mujeres o que en algunos casos, aunque existe, no tiene las atribuciones que le facultan para coordinar una política nacional. Es deseable que la redacción de la ley al listar las responsabilidades del Estado no sugiera, sino obligue. Las capacitaciones especializadas a personal encargado de la administración de justicia, educación y seguridad deben establecer entre sus temarios la creación de protocolos, rutas de acción o estrategias de prevención que puedan ser viables para su implementación. Las campañas de sensibilización pueden priorizar los espacios educativos formales y no

	<p>sector privado, sociedad civil y comunidad técnica. Esta mesa se reunirá de manera periódica para coordinar acciones y desarrollar estrategias conjuntas de gobernanza digital abierta, inclusiva, transparente y con perspectiva de género;</p> <p>b. Implementar medidas 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;</p> <p>c. Asegurar el uso seguro de internet, la prevención de la violencia de género y el cierre de la brecha digital, garantizando que las mujeres en situaciones de vulnerabilidad tengan igual acceso para utilizar las tecnologías de manera efectiva;</p>	<p>b. Incorporar la educación y alfabetización digital en todos los niveles del currículo educativo,</p> <p>c. Garantizar el acceso equitativo y responsable a la tecnología digital, fomentando la participación activa y segura de las mujeres, niñas y adolescentes en el entorno digital;</p> <p>d. Empezar acciones con el objetivo de cerrar la brecha digital, garantizando que las mujeres en situaciones de vulnerabilidad tengan igual acceso para utilizar las tecnologías de manera efectiva;</p>	<p>formales, pero también pueden adaptarse de manera integral a otros ámbitos comunitarios como los espacios culturales, recreativos o deportivos que no implican una estructura de formación, adiestramiento, entrenamiento o aprendizaje sino espacios de convivencia y sinergia con poblaciones que pueden estar en riesgo como son los y las adolescentes y jóvenes.</p>
Artículo 10, inciso e	Se establece que las autoridades actuarán “de oficio”		Este artículo es positivo en términos de protección y prevención, especialmente en entornos como Telegram, donde operan redes de explotación. Sin embargo, requiere una homologación legislativa nacional en todos los países firmantes. Implica una fuerte carga legislativa para cada Congreso nacional.
Artículo 15	“Los proveedores deberán designar a una persona representante en cada país...”		Esta disposición es positiva y necesaria, ya que facilitará la obtención de pruebas para judicializar casos. Sin embargo, los países deberán adecuar sus leyes de telecomunicaciones para obligar a las plataformas a designar a estas personas en su territorio.
Artículo 20 Mecanismos internos de denuncia	<p>Los proveedores de servicios deberán implementar sistemas internos que permitan a las personas usuarias denunciar contenidos que vulneren los derechos protegidos por esta Ley y solicitar su eliminación, suspensión o restricción. Adicionalmente, deberán garantizar la existencia de canales no automatizados que permitan a las personas usuarias solicitar una segunda revisión en caso de no recibir</p>	<p>Los proveedores de servicios deberán implementar sistemas internos que permitan a las personas usuarias denunciar contenidos que vulneren los derechos protegidos por esta Ley y solicitar su eliminación, suspensión o restricción de forma ágil y libre de revictimización.</p> <p>Adicionalmente, deberán garantizar la existencia un contacto humano, no canales automatizados, que permitan a</p>	Debe ser fácil e identificable los mecanismos de denuncia de contenidos, sin tener que leer páginas extensas o instrucciones complicadas.

	<p>una respuesta satisfactoria. Estos mecanismos deberán ser accesibles, gratuitos y garantizar una respuesta rápida, oportuna y fundamentada. Las denuncias deberán ser evaluadas de manera no discriminatoria, diligente y ajustada a los principios establecidos en esta Ley y a los estándares de derecho internacional.</p>	<p>las personas usuarias solicitar una segunda revisión y argumentar su petición, en caso de no recibir una respuesta satisfactoria.</p> <p>Estos mecanismos deberán ser accesibles, gratuitos y garantizar una respuesta rápida, oportuna, transparente y fundamentada. Las denuncias deberán ser evaluadas de manera no discriminatoria, diligente y ajustada a los principios establecidos en esta Ley y a los estándares de derecho internacional.</p> <p>Los mecanismos de denuncia para las personas usuarias deberán de estar siempre visibles y disponibles</p>	
Artículo 21	<p>Cuando el punto de contacto con las autoridades del Estado reciba una orden de actuación de las autoridades judiciales o administrativas nacionales competentes contra uno o varios elementos de contenido reconocidos en la presente ley, o solicitudes para proporcionar información específica sobre una o varias personas usuarias, deberá:</p> <p>a. Actuar sin demora frente a la solicitud de la autoridad correspondiente;</p> <p>b. Informar por escrito a la autoridad que emitió la orden, o a cualquier otra autoridad especificada en la misma, sobre las acciones y las fechas en que fueron realizadas.</p>	<p>Cuando el punto de contacto con las autoridades del Estado reciba una orden de actuación de las autoridades judiciales o administrativas nacionales competentes contra uno o varios elementos de contenido reconocidos en la presente ley, o solicitudes para proporcionar información específica sobre una o varias personas usuarias, deberá:</p> <p>a. Actuar sin demora frente a la solicitud de la autoridad correspondiente;</p> <p>b. Informar por escrito a la autoridad que emitió la orden, o a cualquier otra autoridad especificada en la misma, sobre las acciones y las fechas en que fueron realizadas.</p> <p>c. Verificar que la orden o solicitud provenga de una autoridad competente conforme a la legislación nacional aplicable, y que esté debidamente fundada y motivada en los principios de legalidad, necesidad y proporcionalidad;</p> <p>d. Documentar detalladamente el procedimiento seguido, incluyendo la fecha y hora de recepción de la orden, la identidad de la persona funcionaria que la emitió, las acciones tomadas, las personas responsables de su cumplimiento y los tiempos de respuesta;</p>	<p>Se busca garantizar que las órdenes de autoridades sobre contenidos o datos de personas usuarias se atiendan de forma legal, transparente y con respeto a los derechos humanos con el fin de no perjudicar los procesos judiciales nacionales. Se establecen procedimientos claros para verificar la legalidad de las solicitudes, documentar las acciones y auditorías futuras.</p>

		<p>e. Conservar copia íntegra de la orden y del expediente relacionado durante un plazo mínimo de cinco años, para fines de auditoría, rendición de cuentas o defensa legal;</p> <p>f. Elaborar y publicar informes estadísticos, de forma agregada y periódica, que incluyan el número de órdenes y solicitudes recibidas, su tipología, las autoridades emisoras, y el porcentaje de cumplimiento, con el objeto de garantizar la transparencia y la rendición de cuentas.</p>	
Artículo 22	<p>Los proveedores de servicios que utilicen algoritmos deberán diseñarlos y gestionarlos de manera transparente, ética y accesible en los idiomas locales y con pertinencia cultural. Además, deberán proporcionar términos de servicio claros que permitan a las personas usuarias tomar decisiones informadas sobre el uso de sus servicios, así como otorgar o retirar su consentimiento de manera consciente. Los proveedores de servicios intermediarios deberán implementar opciones que otorguen mayor control a las personas usuarias sobre su experiencia. Estos algoritmos deberán incorporar la prevención de la violencia digital contra las mujeres por razones de género, minimizar la amplificación de contenidos dañinos y eliminar sesgos y estereotipos que perpetúan la violencia, garantizando un entorno digital que respete y proteja los derechos humanos.</p>	<p>A través de la presente Ley, se mandata la creación, entrada en vigor y cumplimiento de un protocolo nacional para la transparencia algorítmica, mismo que establezca mecanismos de transparencia y rendición de cuentas, así como consecuencias por desacato o incumplimiento.</p> <p>Los proveedores de servicios que utilicen algoritmos deberán diseñarlos y gestionarlos de manera transparente, ética y accesible en los idiomas locales y con pertinencia cultural. Además, deberán proporcionar términos de servicio claros que permitan a las personas usuarias tomar decisiones informadas sobre el uso de sus servicios, así como otorgar o retirar su consentimiento de manera consciente. Los proveedores de servicios intermediarios deberán implementar opciones que otorguen mayor control a las personas usuarias sobre su experiencia. Estos algoritmos deberán incorporar la prevención de la violencia digital contra las mujeres por razones de género, minimizar la amplificación de contenidos dañinos y eliminar sesgos y estereotipos que perpetúan la violencia, garantizando un entorno digital que respete y proteja los derechos humanos.</p>	<p>Esta Ley debe mandatar la elaboración de protocolos y programas, así como la creación de entidades o instituciones que habiliten su pleno cumplimiento.</p>
Artículo 28	<p>El Ministerio de Justicia, en coordinación con el Ministerio Público y los mecanismos nacionales competentes, deberán garantizar a las mujeres víctimas</p>	<p>El Ministerio de Justicia, en coordinación con el Ministerio Público y los mecanismos nacionales competentes, deberán garantizar a las mujeres víctimas y</p>	<p>Brindar la facultad de que pueda ser informada una posible víctima de violencia digital a través de las plataformas.</p>

	y sobrevivientes y a sus familiares, los siguientes derechos, a través de la creación de directrices específicas: (...)	sobrevivientes y a sus familiares, los siguientes derechos, a través de la creación de directrices específicas: (...) f. Cuando se identifique que un perfil podría estar en riesgo de ser víctima de violencia digital, la persona usuaria deberá ser notificada oportunamente por medio de la plataforma digital correspondiente.	
Artículo 30	Artículo 30. Medidas cautelares El Tribunal Competente podrá imponer medidas cautelares a petición del Ministerio Público, de la víctima o la representación de la víctima, en los casos previstos por esta Ley. En caso de que soliciten una medida cautelar durante el plazo establecido por la ley, dicha cuestión deberá resolverse inmediatamente después de formulada la imputación. Para tal efecto, las partes podrán ofrecer aquellos medios de prueba pertinentes para analizar la procedencia de la medida solicitada.	Artículo 30 Bis o 31.	Es importante establecer un apartado que aborde las medidas de protección disponibles para las víctimas. Cabe señalar que dichas medidas no dependerán de la apertura de una carpeta de investigación. Será suficiente con que la víctima se presente en los Centros de Justicia para las Mujeres o instancia equivalente, para notificar el hecho delictivo, a partir de esa notificación, se procederá a ordenar las medidas de protección correspondientes. En cuanto al artículo 30, que establece que 'deberá resolverse inmediatamente después de formulada la imputación', surge la interrogante de qué sucederá con aquellas víctimas que: A) deciden no denunciar B) Su carpeta no se logra vincular.
Artículo 31	Artículo 31. Tipos de medidas cautelares El/la juez/a podrá dictar, de forma razonada, una o varias de las siguientes medidas cautelares para proteger a la víctima y garantizar el desarrollo adecuado del proceso judicial: a. Prohibir al imputado acercarse físicamente a la víctima o comunicarse con ella por cualquier medio, incluido aquellos disponibles en el entorno digital. Esta prohibición se extenderá a las personas bajo el cuidado o protección de la víctima;	Artículo 31. Tipos de medidas cautelares El/la juez/a podrá dictar, de forma razonada, una o varias de las siguientes medidas cautelares para proteger a la víctima y garantizar el desarrollo adecuado del proceso judicial: a. Prohibir al imputado acercarse físicamente a la víctima o comunicarse con ella a través de interpósita persona o por cualquier medio, incluido aquellos disponibles en el entorno digital, como redes sociales, correos electrónicos, mensajes de texto, aplicaciones de mensajería instantánea y cualquier otra plataforma que facilite la comunicación. Esta prohibición se extenderá a las personas bajo el cuidado o protección de la víctima; c) En los casos en que el agresor y la víctima compartan espacios	Se incluye la comunicación a través de terceros, familiares, amistades. Se especifica el entorno digital para no dejar ambigüedades. Se otorga el beneficio a la víctima y el agresor debe ser retirado de los espacios en los que converjan, en tanto no exista una resolución definitiva.

		de convivencia, tales como los entornos laborales o educativos, se deberá aplicar una medida cautelar que restrinja temporalmente el acceso del agresor a dichos espacios. La víctima no estará obligada a abandonar dichos entornos, y podrá continuar en ellos hasta que se emita una sentencia definitiva en el proceso.	
Artículo 34	“Las acciones descritas en el artículo 7... deberán ser tipificadas como delitos de acción pública, sin que ello constituya una lista exhaustiva o limitada.”		Esta redacción rompe con el principio de legalidad penal y exacta aplicación de la ley, ya que no puede haber delitos por analogía ni aplicación extensiva del tipo penal. La ley penal debe ser estricta, taxativa y clara en su redacción.
Artículo 38	“Obstaculización del acceso a la justicia...”		Es positivo que se reconozca esta conducta como sancionable. Podría reforzarse agregando ejemplos de prácticas comunes de obstaculización digital, como ignorar solicitudes judiciales o dilatar respuestas intencionalmente.
Artículo 39	“No podrán considerarse eximentes la emoción violenta...”		El documento confunde elementos de teoría del delito, ya que la emoción violenta sí puede constituir, en ciertos casos, un trastorno mental transitorio, que afecta la imputabilidad. No puede eliminarse de forma tajante sin atender a estudios médicos o criminológicos.
Artículo 43	“Destinación de recursos provenientes de sanciones...”		Se propone mejorar este apartado agregando mecanismos de vigilancia y transparencia ciudadana sobre el uso de los recursos recaudados, así como claridad sobre qué instituciones los administrarán.
Artículo 44. Responsabilidad civil de los proveedores de servicios	En los procesos de responsabilidad civil, los jueces y juezas estarán facultados para evaluar los actos que tengan como propósito o resultado manifestaciones de violencia digital contra las mujeres por razones de género, atribuibles a cualquier persona física o jurídica en el marco de esta ley. Cuando así lo determinen, conforme a las disposiciones legales vigentes, podrán aplicar las sanciones contempladas en el artículo 42 de la presente Ley.		De existir leyes vigentes en materia de regulación de proveedores de servicios digitales, se debe referir a ese instrumento y quizás hacer las reformas adecuadas para ampliar o especificar las responsabilidades de las empresas dueñas de plataformas digitales, de streaming, aplicaciones, proveedores de internet, etc. Es deseable que se incluyan obligaciones de constitución o de que exista una persona representante en el territorio nacional y que se cumpla con las

	Las víctimas tendrán el derecho de exigir responsabilidad civil por acciones u omisiones constitutivas de violencia digital contra las mujeres que, aunque no estén tipificadas como delito, vulneren sus derechos, especialmente aquellos consagrados en la Convención de Belém do Pará.		responsabilidades fiscales del país, así como el pleno cumplimiento con la legalidad del país en donde operen, sin importar que estén constituidas en otro país. Para apoyar la afirmación de que las “víctimas tendrán derecho”, se puede especificar que el Estado debe asegurar los mecanismos institucionales para garantizarlo, así como consecuencias frente a la violación de dicho derecho y mecanismos de reparación del daño a las personas vulneradas.
Artículo 45 Responsabilidad de las personas jurídicas	La persona jurídica que participe directa o indirectamente en la comisión de los delitos previstos en esta ley podrá responder civil o administrativamente, según corresponda, sin perjuicio de la responsabilidad penal que recaiga sobre las personas físicas involucradas. Se considerará responsable a la persona jurídica en los siguientes casos: a. Cuando el delito sea cometido por una persona que desempeñe funciones directivas o de representación en la empresa. b. Cuando el delito sea cometido por una persona física que actúe siguiendo instrucciones de una persona con funciones directivas o de representación.	La persona jurídica/ moral que participe directa o indirectamente en la comisión de los delitos previstos en esta ley podrá responder civil o administrativamente, según corresponda, sin perjuicio de la responsabilidad penal que recaiga sobre las personas físicas involucradas. Se considerará responsable a la persona jurídica/ moral en los siguientes casos: a. Cuando el delito sea cometido por una persona que desempeñe funciones directivas o de representación en la empresa. b. Cuando el delito sea cometido por una persona física que actúe siguiendo instrucciones de una persona con funciones directivas o de representación. c. Cuando la persona jurídica/moral cuente entre sus giros alguna actividad que vaya en detrimento de la seguridad, dignidad y bienestar integral de las mujeres. Como es el caso de los mercados de explotación sexual digitales.	Resaltar la responsabilidad de los sitios web, páginas y empresas cuya actividad principal es la explotación de la imagen hipersexualizada de mujeres y otras poblaciones sin su consentimiento. Ejemplo: páginas de “pornografía casera” en las que no se tienen controles suficientes para identificar el pleno consentimiento de todas las personas cuya imagen es expuesta y garantizar la plena reparación en caso de daños y perjuicios.

NOTAS ADICIONALES

- 1) Se sugiere una aclaración de la equivalencia que puede haber entre Ministerios y Secretarías o instancias responsables de algún tema a nivel nacional, considerando las diferencias políticas de cada país.
- 2) CAPÍTULO II - Se hace referencia únicamente a “Deberes del Estado” - El Estado es parte vital en materia de prevención de la violencia digital, sin embargo, pueden existir otros órganos reguladores más allá de los estipulados, por ejemplo, facilitar mecanismo de democratización, es decir, más acceso a participación en acciones y toma de decisiones en temas de prevención para la sociedad civil, se puede agregar un capítulo sólo para la inclusión de organizaciones, colectivos o actores clave en la prevención de la violencia digital.
- 3) La participación ciudadana es un pilar importante en la prevención de la violencia porque se involucran actores clave como activistas, padres, madres o tutores, personal docente en las escuelas, autoridades y funcionarios locales, entre otros, las medidas comunitarias tienen un mayor alcance hacia poblaciones con indicadores de vulnerabilidad mayormente establecidas en zonas conurbanas, rurales y semi rurales.
- 4) **Tipologías de violencia digital (sólo como insumo, hay algunas que ya están abordadas, pero otras que faltan)**
 - a. Exclusión virtual - limitaciones al acceso al uso de los espacios virtuales impuestas por condiciones estructurales diversas, entre las que se pueden encontrar: el ingreso, la escolaridad, la localización geográfica, la edad, el ser parte de un grupo sociodemográfico vulnerable, etc. También se puede tratar de limitaciones impuestas por la censura de la plataforma, página o espacio virtual del que se trate, sobre una persona o grupo en particular por sus posiciones políticas, ideológicas, etc. Existe también la autoexclusión cuando se ha sido víctima de ataques y violencias en los espacios virtuales, que obligan a retirarse parcial o totalmente de los mismos por cuestiones de seguridad. La exclusión de personas o grupos de los espacios virtuales agrava las brechas y desigualdades sociales existentes.
 - b. Insultos electrónicos - expresiones emitidas por medios digitales que tienen la intención de ofender, denigrar, causar malestar y molestar a alguien.
 - c. Violación de datos personales - pérdida, alteración, destrucción o difusión no consentida, accidental o ilícita de datos o información personales en posesión de una persona física o moral. También puede incluir el acceso no autorizado a comunicaciones privadas o a cuentas y perfiles de otras personas.
 - d. Asecho / Stalking - persecución, vigilancia y/o asecho obsesivo de las actividades virtuales de una persona.
 - e. Hostigamiento virtual - conductas violentas, ofensivas y de maltrato, constantes y reiteradas contra una persona o grupo de personas a través de redes sociales u otras vías de comunicación en la virtualidad. Pueden ser de carácter sexual o no.
 - f. Suplantación virtual - apropiación indebida, comúnmente malintencionada y sin consentimiento de la identidad digital de otra persona. Puede ser a través del uso de su imagen u otros datos para la creación de perfiles falsos, o del acceso no autorizado a sus cuentas o perfiles, para fines diversos que suelen resultar en perjuicio de la persona cuya identidad fue suplantada.

- g. Difamación virtual - Uso de medios digitales para emitir una acusación o denuncia falsa o desproporcionada de una persona para dañar su reputación, imagen, dignidad u honor en perjuicio de sus vínculos, medios de subsistencia, entre otras afectaciones.
- h. Ciberpersecución - Serie de conductas por medio de las que una persona busca hacerse presente para otra a través de todas las vías digitales posibles (en sus diferentes redes sociales, canales, cuentas y otros espacios que utilice en la virtualidad), de forma reiterada, insistente, hostigadora y/o amenazante a pesar de que las comunicaciones no sean correspondidas.
- i. Sextorsión - práctica a través de la cual se busca manipular, controlar, obligar o inducir a una persona a determinada conducta, bajo la amenaza de que, si no obedece, su contenido íntimo-sexual, será difundido. Se suele pedir dinero, más material íntimo, encuentros sexuales, etc.
- j. Difusión de contenido íntimo sin consentimiento - dar a conocer por cualquier medio, por cualquier vía y a cualquier persona o grupo de personas, contenido íntimo (particularmente erótico – sexual) de una persona, sin que esta lo haya consentido o autorizado específica y explícitamente.
- k. Trata virtual de personas - explotación de personas con el uso de medios digitales y de la virtualidad. Se suele presentar a modo de catálogos de prostitución en línea, revelando ubicación y/o vías de contacto de personas a quienes se ofrece para su explotación sexual o de cualquier otro tipo, usurpando la identidad de las personas y vendiendo contenido sexual (que puede corresponder o no a la persona cuya identidad se alude) sin consentimiento, entre otras formas.

(Fuente: Oropa Marcela, et. al. (2022), Informe Violencia Digital. Un estudio de los perfiles de agresores y sobrevivientes de violencia sexual digital. Frente Nacional para la Sororidad y Defensoras Digitales. México 2022)

5) Tipologías de violencia sexual digital (sólo como insumo, hay algunas que ya están abordadas, pero otras que faltan)

- a. Producción no consentida de material íntimo sexual: grabar o fotografiar sin consentimiento un encuentro sexual o la desnudez total o parcial de alguien inconsciente o que no ha dado su consentimiento. Por ejemplo, grabar por debajo de la falda o a través de cámaras ocultas en vestidores y/o baños, etc. Esto incluye también la elaboración de imágenes o videos sexuales o de desnudos, con la identidad de alguien (sin su autorización) por medio del uso de tecnologías digitales, incluyendo la inteligencia artificial (deepfakes).
- b. Difusión de contenido íntimo-sexual sin consentimiento, como fotografías, imágenes editadas, videos, o audio. Esta forma de VSD se puede perpetrar en casos en los que el contenido se haya obtenido de forma consensuada (en un contexto de sexting, en una sesión fotográfica, etc.) o no (ver el punto anterior, así como a través del acceso no autorizado a cuentas o chats ajenos).
- c. Robo o usurpación de la identidad con fines de explotación sexual, al usar una identidad ajena para la difusión y/o venta de contenido sexual, ya sea que este pertenezca realmente o no a la persona cuya identidad es aludida (también conocido como prostitución virtual).
- d. Acoso sexual digital, por ejemplo, al enviar fotografías sexuales y/o mensajes obscenos o lascivos sin que sean solicitados ni haya consentimiento para recibirlos. Puede o no estar acompañado de amenazas.

- e. Grooming o el fingir una identidad virtual distinta a la real para vincularse con personas menores de edad hasta crear un lazo de confianza y después manipularles para realizar actos que pueden poner en peligro su integridad, seguridad, bienestar o intimidación sexual.
- f. Sextorsión o el exigir dinero, material íntimo, encuentros sexuales, videollamadas sexuales, etc. a cambio de no difundir contenido íntimo de otra persona.
- g. Amenazas, ya sea manipulando, controlando, obligando o induciendo a una persona a determinada conducta, bajo la amenaza de que, si no obedece, su contenido íntimo-sexual, será difundido o que sufrirá un ataque sexual físico.
- h. Acecho o la persecución y vigilancia continua a través de redes y dispositivos digitales, busca coartar la libertad de la víctima y ejercer control sobre sus acciones.
- i. Ofrecimiento de servicios sexuales no autorizados como a través de la creación de catálogos de prostitución en línea, los cuales usurpan identidades personas y ofrecen —sin su consentimiento— servicios sexuales en su nombre y venden contenido sexual (el cual puede corresponder, o no, a la persona aludida). Estos anuncios suelen ir acompañados de los datos personales de la persona cuya identidad se expone.

Fuente: Hernández Oropa, M., Chavarría García, P.I., Contreras Chávez, I., et al. (2024) “Violencia sexual digital contra las mujeres en México: El papel de Ley Olimpia en la transformación de los mandatos de género que la sostienen”. ALIGN Informe. Londres: ALIGN/ODI

(www.alignplatform.org/resources/report-digitalsexual-violence-against-women-mexico-olimpia-law) .pg. 14 <https://leyolimpia.com.mx/wp-content/uploads/2024/10/fns-mexico-digitalsexualviolence-report-spanish.pdf>

- 6) No creemos que los ataques digitales de género contra las mujeres se “facilitan por las tecnologías” porque esta expresión da a entender que las plataformas digitales y por lo tanto las empresas detrás de ellas, son solo herramientas neutras, evitando visibilizarlas como actores corresponsables de una violencia real y sistémica. Además de que, desde el reconocimiento de lo digital como un ámbito de existencia humana, con todas las complejidades y profundidades que eso conlleva, resulta coherente y lógico nombrar la violencia digital así, como una modalidad, tal como se nombra la violencia escolar, familiar, laboral, sin términos rebuscados y complejos que finalmente no comunican en el uso del lenguaje cotidiano lo que se quiere nombrar. No se habla de “violencia de género facilitada por las aulas de clases/los centros laborales/ la vía pública/ los hogares”, porque sería impreciso. Lo mismo sucede con el concepto de “Violencia de género facilitada por las tecnologías”. Y si ese concepto se acuñó sin entender la digitalidad como un ámbito, se le entendió entonces como una herramienta neutra (lo que ya desmontamos) e igualmente resultaría impreciso hablar de “violencia de género facilitada por las armas/el ácido/los autos”. De tal modo que sostenemos la congruencia de defender una terminología correcta para fines jurídicos y legislativos.

FIRMAS

