Este documento presenta los comentarios de Derechos Digitales a la Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia Digital contra las Mujeres por Razones de Género. Derechos Digitales es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005, cuyo objetivo fundamental es el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. La violencia de género facilitada por la tecnología ha sido un foco importante del trabajo de la organización en los últimos años, y nuestra contribución se basa en esta experiencia.

En este documento, presentamos nuestros puntos de atención con respecto a la versión de la Ley Modelo enviada en febrero de 2025. Aquí, exponemos brevemente nuestras preocupaciones sobre artículos específicos y, en algunos casos, sugerimos ajustes a su redacción.

- **Artículo 1. Objeto**

Las mujeres han enfrentado históricamente violencia de género, tanto en el ámbito digital como fuera de él. Es fundamental que la ley establezca una definición amplia de mujeres que incluya explícitamente a todas las personas que así se auto perciban. A su vez, consideramos que la ley también debería incluir en su ámbito de protección a personas que se identifican como LGBTQIA+, quienes también son víctimas/sobrevivientes[1] de violencia por razones de género.

Es importante señalar que, aunque el abordaje hacia la violencia de género se ha centrado principalmente en las mujeres y las niñas cis, dado que las normas de género también afectan a la orientación sexual y la expresión de género, las personas LGBTQIA+ también se ven afectadas por la violencia de género, incluyendo cuando ésta se ve facilitada por la tecnología.[2] La violencia de género está profundamente arraigada en la imposición de normas patriarcales sobre género y sexualidad. Este tipo de violencia busca castigar y controlar a quienes desafían las expectativas tradicionales de identidad y expresión de género. Las personas trans, no binarias y los hombres gays, por ejemplo, suelen ser víctimas/sobrevivientes de agresiones físicas, psicológicas y digitales, pues sus identidades son vistas como una amenaza a la estructura patriarcal[3]. A modo de ejemplo, las personas LGBTQIA+ pueden ser objeto de violencias específicas como violaciones correctivas, exposición forzada de su identidad ("outing"), chantajes con imágenes íntimas y campañas de odio organizadas en línea. Por ello, consideramos esencial que las leyes contra la violencia de género incluyan explícitamente la protección de las personas LGBTQIA+, garantizando un enfoque más inclusivo y efectivo en la lucha contra esta forma de violencia.

---

[1] Los términos son usados indistintamente en este documento y responden a la identificación de la propia persona como tal

[2] Suzie Dunn. (2021)"Technology-facilitated Gender-Based Violence-An Overview" CIGI Supporting a Safer Internet Paper No. 1. Online: https://www.cigionline.org/static/documents/SaferInternet_Paper_no_1_coverupdate.pdf

[3] Ibid

Sugerencia de nueva redacción: “Esta ley tiene por objeto la prevención, atención, protección, investigación, sanción, reparación de los daños y erradicación de la violencia digital contra las mujeres en toda su diversidad **y personas LGBTQIA+** por razones de género, instigada, mediada o con el uso de las tecnologías, abarcando tanto los actos de violencia digital como aquellos perpetrados con el uso o a través de las tecnologías, tanto en el ámbito público como privado.”

- **Artículo 2. Definición**

Una definición de VG FT no debe depender exclusivamente de la constatación de un daño físico, psicológico o económico inmediato, ya que muchas de sus manifestaciones tienen impactos amplios, duraderos y multidimensionales. Por ello, es fundamental que la definición legal contemple formas de violencia que afecten otros aspectos de la vida y los derechos de las personas.

Además, muchas manifestaciones de VG FT evolucionan de forma constante, generando nuevas formas de daño y afectación. El uso de la tecnología, por su carácter dinámico y cambiante, da lugar a agresiones que no siempre se encuadran fácilmente en categorías jurídicas tradicionales. En consecuencia, una definición legal debe ofrecer una protección amplia que considere no solo los efectos materiales de la violencia, sino también sus impactos sobre otros derechos fundamentales.

La definición adoptada por ONU Mujeres ofrece un marco sólido para avanzar en ese sentido, al señalar que la VG FT puede incluir: “*any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools which results in or is likely to result in physical, sexual, psychological, social, political or economic harm or* ***other infringements of rights and freedoms***”[4].

En relación con el artículo 2 de la Ley Modelo, también se sugiere —a partir de la definición de VG FT propuesta por UNFPA en 2023— el uso del término “basado en el género”, sin una mención específica o excluyente a las “mujeres”: “*an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media,* ***against a person on the basis of their gender***”[5].

Por las razones expuestas en la sección anterior de este documento, esta perspectiva permite incorporar de forma explícita la mención a que este tipo de violencia se basa en el género, sin restringir su aplicación a categorías identitarias determinadas, lo que garantiza mayor precisión normativa y coherencia con los estándares internacionales de derechos humanos.

---

[4] UN WOMEN (2025). FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women. Online: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

[5] UNFPA (2023). Brochure: What is technology-facilitated gender-based violence? Online: https://www.unfpa.org/resources/brochure-what-technology-facilitated-gender-based-violence

Sugerencia de nueva redacción: “Cualquier acción, conducta u omisión **contra una persona**, basada en su género, que cause muerte, daño, o sufrimiento físico, sexual, psicológico, económico o simbólico, **o que afecte de otras maneras sus derechos y libertades**, en cualquier ámbito de su vida, que sea cometida, instigada o agravada, en parte o en su totalidad, con el uso de las tecnologías.”

- **Artículo 3. Ámbito de aplicación**

Es importante incluir en este artículo que la ley debe contemplar, al lado de la de los Estados, la responsabilidad de agentes privados, como empresas y otras personas jurídicas, que pueden no solo cometer directamente actos de VG FT, sino también contribuir a ellos por omisión. Eso se basa directamente en los Principios Rectores sobre las Empresas y los Derechos Humanos.

Además, la inclusión es coherente con lo que la ley ya reconoce en su Capítulo III, y se justifica por el hecho de que plataformas digitales, redes sociales y proveedores de servicios de internet han fallado sistemáticamente en adoptar medidas adecuadas para prevenir y sancionar esta forma de violencia. La falta de medidas claras sobre la responsabilidad de estos actores ha permitido que las agresiones digitales se multipliquen sin una respuesta efectiva, lo que torna esencial que la ley establezca obligaciones precisas para quienes faciliten, toleren o no actúen frente a la VG FT[6].

Sugerencia de redacción:
“Se entenderá que la violencia digital contra las mujeres por razones de género incluye aquella: (...)
b. Que tenga lugar en la comunidad y sea perpetrada por cualquier persona, **independientemente de sua identificação ou identificabilidade**.
(...)
d. Que sea perpetrada, tolerada, con complicidad o aquiescencia de agentes privados, ya sea por la ausencia de políticas de protección y prevención, por inacción ante reportes 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 4. Princípios Rectores**

Una ley sobre VG FT debe incluir la interseccionalidad entre sus principios rectores, ya que esta forma de violencia afecta a diferentes grupos de manera desproporcionada, profundizando desigualdades preexistentes. Personas LGBTQIA+, personas racializadas,

[6] Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls, A/HRC/38/47, 18 June 2018; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/76/258, 30 July 2021.

con discapacidad y otros grupos en situación de vulnerabilidad suelen experimentar impactos diferenciados y más severos de la VG FT, debido a formas estructurales de discriminación en nuestra sociedad, como el racismo, el capacitismo y la desigualdad socioeconómica[7].

La interseccionalidad expresamente reconocida como principio rector permite que la ley reconozca y aborde estas diferencias, asegurando que las políticas públicas y las medidas de protección sean realmente efectivas para todas las víctimas/sobrevivientes, sin importar su identidad de género, orientación sexual, condición socioeconómica u otros marcadores de opresión. Este enfoque permite no solo dimensionar los impactos diferenciados, sino construir políticas públicas efectivas que garanticen una protección a las poblaciones mayormente vulnerabilizadas.

Sugerencia de redacción: “Los principios rectores de esta ley reconocen que el derecho de las mujeres a vivir libres de violencia digital es una responsabilidad conjunta del Estado y los proveedores de servicios, y para ello debe garantizarse: (...) **b. Interseccionalidad**”

- **Artículo 5. Definiciones**

a. Sesgo o prejuicio algorítmico

Se sugiere precisar que el sesgo o prejuicio algorítmico no es solamente el resultado de errores técnicos o de funcionamiento del sistema, sino que también puede derivarse directamente de los datos utilizados para entrenar los modelos algorítmicos. Estos datos, al estar muchas veces marcados por patrones históricos de desigualdad, pueden incorporar sesgos de género, raza, orientación sexual u otros factores estructurales que terminan reproduciéndose —e incluso amplificándose— en las decisiones automatizadas.

En este sentido, se recomienda que la definición contemple que el sesgo algorítmico también tiene su origen en las decisiones humanas sobre qué datos se producen, seleccionan, cómo se estructuran y qué objetivos se programan. Incluir esta dimensión permitiría una comprensión más integral del fenómeno y fortalecería las obligaciones de prevención y auditoría por parte de los desarrolladores y operadores de estas tecnologías.

c. Moderación de contenidos

La definición de moderación de contenido debe ser más amplia e incluir explícitamente la configuración de los algoritmos que estructuran plataformas como las redes sociales, así como las prácticas de curación de contenidos. La curación se refiere a la selección y organización de contenidos realizada por las plataformas para moldear la

[7] Dunn, S. (2022). Addressing Gaps and Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Gender-based Violence. UN Women.

experiencia informativa y comunicativa de las personas usuarias, lo cual tiene implicaciones directas sobre qué discursos se visibilizan o se silencian.

Las decisiones automatizadas de las plataformas influyen directamente en qué tipos de contenido serán impulsados, suprimidos o eliminados. La moderación y la curación no ocurren únicamente a través de la eliminación de publicaciones, sino también mediante la jerarquización de lo que es visible y accesible, por ejemplo, mediante recomendaciones, tendencias o algoritmos de búsqueda. Muchas veces, los contenidos violentos o misóginos no sólo no son eliminados, sino que son priorizados y amplificados por estos sistemas.

Por ello, el artículo debe ampliarse para abarcar también la responsabilidad de las plataformas en la configuración algorítmica y la definición de sus criterios editoriales, garantizando que no perpetúen ni amplifiquen la violencia digital de género mediante la lógica de la interacción, el alcance o el engagement.

En este sentido, puede retomarse -y se sugiere el uso de- la definición incluida en el informe del Relator Especial de la ONU para la libertad de expresión, David Kaye, de 2018. Su enfoque reconoce que la moderación y la curación son procesos integrados e inseparables en los entornos digitales contemporáneos, y que su regulación requiere una mirada centrada en derechos humanos, con enfoque de género, transparencia y rendición de cuentas. El señala que: "*La moderación de contenidos comprende una amplia gama de actividades: la eliminación de contenido ilegal, ofensivo o indeseado; la clasificación y priorización de la información mostrada; así como la curación algorítmica de contenidos en función de intereses comerciales o ideológicos*"[8].

e. Desinformación o difusión de contenidos falsos

En español aún no existe un término consensuado y ampliamente utilizado para traducir *misinformation*, por lo que se mantiene el uso del término en inglés para distinguirlo claramente de *disinformation*, que sí tiene traducción habitual como "desinformación".

La redacción actual del artículo 8e genera confusión entre ambos conceptos. Mientras que *disinformation* se refiere a la difusión deliberada e intencional de contenidos falsos con el objetivo de causar daño, *misinformation* describe la difusión de información errónea sin intención ni conocimiento de su carácter. Sin embargo, el texto del artículo trata ambas conductas como si fueran dolosas, lo que genera una imprecisión conceptual preocupante, especialmente cuando esta tipificación puede ser invocada en contextos políticos sensibles.

Además, el artículo 8c, al tipificar como violencia política de género la "difusión de contenidos falsos", refuerza esta ambigüedad y corre el riesgo de criminalizar acciones que no tienen intención de causar daño, abriendo margen para arbitrariedades.

En este sentido, el informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, ofrece una definición que puede ser útil para orientar la formulación normativa: "*La desinformación [disinformation] ha*

[8] A/HRC/38/35. Online: https://documents.un.org/doc/undoc/gen/g18/096/75/pdf/g1809675.pdf

estado presente desde hace milenios, pero ha vuelto a cobrar aceptación en la era digital. Aunque no existe una definición única y consensuada de "desinformación", este término se utiliza cada vez más para referirse a la manipulación de información falsa o que conduce a error para engañar intencionadamente y causar daño a la población. Conviene distinguirla de la información errónea [misinformation], que es una falsedad difundida sin intención de causar daño"[9].

También es importante advertir sobre el mal uso de legislaciones que penalizan la desinformación, especialmente en contextos autoritarios o polarizados. Según el informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación referenciado por un reporte de Derechos Digitales y APC, "*Las leyes supuestamente utilizadas para restringir la desinformación se emplean para silenciar la disidencia, y se invocan la seguridad nacional y el orden público para iniciar procesos penales basados en delitos mal definidos en la legislación sobre ciberdelitos, que a menudo terminan siendo utilizados para reprimir la disidencia y controlar el espacio en línea, así como 'un pretexto para hacer retroceder a la nueva sociedad civil digital'*"[10].

Dichas leyes frecuentemente se conceptualizan sin cumplir con los principios de legalidad, necesidad y objetivo legítimo, ya que los delitos invocados (como desinformación, terrorismo o incitación al odio) no se definen con suficiente precisión ni se establece un vínculo concreto entre el acto cometido y el daño causado. Por ello, recomendamos que la ley tipifique únicamente la conducta dolosa, es decir, la desinformación, y que, en consecuencia, se eliminen los términos "informaciones falsas" tanto del artículo 5e, como del artículo 8c. Además de eso, que esa misma legislación cumpla con esos parámetros, o entonces siga un abordaje no criminal, para no correr el riesgo de criminalizar las voces de grupos vulnerables[11].

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

I. Implementar, diseñar o usar algoritmos, inteligencia artificial, sistemas automatizados de toma de decisiones o herramientas digitales que generen sesgos discriminatorios contra las mujeres por razones de género

Se sugiere revisar la redacción del inciso para incluir no solo los casos en que los sistemas algorítmicos generan sesgos discriminatorios, sino también aquellos en que reproducen o amplifican sesgos ya existentes en los datos o en los contextos sociales en los que operan. Esto permitiría reconocer que muchos de los impactos discriminatorios de las tecnologías no son nuevos, sino que reflejan y profundizan desigualdades estructurales que ya afectan a las mujeres y personas con identidades de género diversas.

---

[9] A/77/288. Online: https://docs.un.org/es/A/77/288
[10] DERECHOS DIGITALES; APC (2023). Online: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf. Ref: A/HRC/41/41. Online: https://docs.un.org/es/A/HRC/41/41
[11] Ibid

Incluir la noción de reproducción de sesgos contribuiría a una definición más precisa y coherente con los estándares internacionales de derechos humanos[12] y con la evidencia empírica existente sobre inteligencia artificial y discriminación algorítmica[13]. Además, ampliaría el alcance normativo del artículo para abarcar situaciones donde las tecnologías perpetúan patrones discriminatorios sin necesariamente haber sido diseñadas con una intención explícita de generar daño.

Sugerencia de redacción: "I. Implementar, diseñar o usar algoritmos, inteligencia artificial, sistemas automatizados de toma de decisiones o herramientas digitales que generen, **reproduzcan o amplifiquen** sesgos discriminatorios contra las mujeres por razones de género".

m. Cualquier otra acción, conducta o acto que tenga como resultado impedir el derecho de las mujeres a estar libres de violencia en el entorno digital

El texto es problemático porque parece limitar las consecuencias de la violencia al entorno digital, sin reconocer que la VG FT genera impactos que también van más allá del espacio online. Este tipo de violencia no solo restringe la participación digital de las víctimas/sobrevivientes, sino que también puede afectar su seguridad física, su vida profesional e incluso su integridad económica y social.

Por ejemplo, casos de acoso en línea pueden derivar en persecuciones en el mundo físico, amenazas digitales pueden llevar al desplazamiento forzado, y la exposición de datos personales puede poner en riesgo la vida de las víctimas/sobrevivientes. Por lo tanto, la definición legal debe reconocer que el impacto de la VG FT no se limita al entorno digital, sino que tiene repercusiones en la vida offline, garantizando así una protección integral y eficaz.

Este enfoque ha sido respaldado por múltiples organismos internacionales que reconocen la violencia facilitada por tecnologías como parte de un *continuum* de violencia de género. La Recomendación General Nº 35 del Comité CEDAW, así como la Resolución 38/5 del Consejo de Derechos Humanos (2018) y el informe A/HRC/38/47 de la Relatora Especial sobre la violencia contra la mujer, subrayan que las formas de violencia en línea deben entenderse como una extensión de las violencias estructurales que históricamente afectan a las mujeres y personas de género diverso. Del mismo modo, la CSW67 reafirma la necesidad de desarrollar marcos normativos que contemplen esta continuidad entre lo digital y lo no digital.

---

[12] En este sentido, destacamos el Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la promoción y protección de los derechos humanos en el contexto de tecnologías digitales, con especial atención a la inteligencia artificial (A/HRC/48/31, 2021), lo cual apunta que los sistemas de IA pueden reproducir y amplificar formas de discriminación existentes y subraya que los Estados y empresas tienen la obligación de garantizar que estas tecnologías respeten los derechos humanos, en particular el principio de no discriminación.

[13] Noble, Safiya Umoja (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*.

Sugerencia de redacción: “m. Cualquier otra acción, conducta o acto **que sea perpetrado por medio de tecnologías de la información y comunicación y** que tenga como resultado impedir el derecho de las mujeres a estar libres de violencia”.

- **Artículos 9, 10, 10bis y 14. Definición de organismos específicos**

Todos estas disposiciones mencionan órganos específicos, ya sean aquellos relacionados con los derechos de las mujeres o aquellos encargados de la regulación de tecnologías, y les otorgan atribuciones en casos de VG FT.

Definir de antemano, en una ley modelo, qué órganos específicos serán responsables de formular políticas y actuar en casos de VG FT puede ser problemático, ya que cada país posee realidades institucionales y regulatorias diferentes, e incluso hay países que podrían no contar con los órganos predefinidos en la ley. Para ilustrar con ejemplos concretos de la región, México está en proceso de eliminar su agencia de protección de datos[14], mientras que Chile recién está estructurando la suya[15] y otros países, como Paraguay, no cuentan con legislación al respecto hasta el momento. Un modelo de ley redactado de esta manera podría ignorar estas diferencias institucionales, volviéndose ineficaz o inviable para su implementación en ciertas jurisdicciones.

Además, la imposición de órganos específicos sin considerar las realidades locales puede abrir espacio para la captura institucional, un fenómeno en el que las agencias reguladoras son influenciadas por intereses políticos o económicos, lo que socava su capacidad de actuar de manera independiente. Uno de los desafíos globales en la regulación del VG FT es precisamente la falta de mecanismos de rendición de cuentas y transparencia en los órganos encargados de proteger los derechos humanos en el entorno digital. Si un país asigna esta función a una entidad vulnerable a la captura regulatoria, esto podría llevar a una implementación ineficaz de la ley, una aplicación selectiva o incluso un uso indebido de las normas para restringir derechos. En Brasil, por ejemplo, la Agencia Nacional de Telecomunicaciones (Anatel), encargada de los temas de telecomunicaciones y con interés en abarcar la regulación de plataformas, ha sido objeto de constantes críticas por parte de la sociedad civil debido a su captura por intereses privados y su alineación con la agenda del sector empresarial[16].

Por ello, lo ideal es que la ley establezca criterios y principios generales para la gobernanza del VG FT, en lugar de designar órganos específicos para esta competencia.

[14] MONDAQ (2025). Extinction Of The National Institute For Transparency, Access To Information, And Personal Data Protection. Online: https://www.mondaq.com/mexico/data-protection/1603734/extinction-of-the-national-institute-for-transparency-access-to-information-and-personal-data-protection

[15] GONZÁLEZ, J. P. (2024). Aspectos del recientemente aprobado proyecto de ley que crea la Agencia de Protección de Datos Personales en Chile. Online: https://iapp.org/news/a/aspectos-del-recientemente-aprobado-proyecto-de-ley-que-crea-la-agencia-de-protecci-n-de-datos-personales-en-chile

[16] COALIZÃO DIREITOS NA REDE (2023). Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel. Online: https://direitosnarede.org.br/2023/04/28/orgao-independente-de-supervisao-das-plataformas-e-essencial-mas-nao-pode-ser-anatel/

De este modo, cada país podría adaptar la implementación de la normativa conforme a sus estructuras institucionales, garantizando así flexibilidad y eficiencia en la lucha contra esta forma de violencia.

- **Artículo 10bis. Medidas de protección de urgencia**

La ausencia de una mención explícita al material en texto en el artículo puede representar una laguna significativa, especialmente considerando que la VG FT no solo ocurre mediante imágenes, videos o audios, sino también a través de textos escritos. Muchas formas de violencia digital contra mujeres y personas LGBTQIA+ se manifiestan a través de mensajes difamatorios, amenazas, acoso sistemático y discurso de odio, los cuales, en muchos casos, se presentan exclusivamente en formato textual.

Por ello, sería recomendable que el artículo explicitara que los materiales en texto también están contemplados, asegurando que todas las manifestaciones de VG FT sean debidamente consideradas, sin importar el formato utilizado por el agresor. Esto fortalecería la coherencia de la legislación y ampliaría la protección de las víctimas/sobrevivientes de violencia digital, garantizando una respuesta legal integral frente a este tipo de agresiones.

Sugerencia de redacción: “Las Comisarías de Familia, los jueces de Control de Garantías del lugar de residencia de la víctima, y órganos judiciales y administrativos con competencia en medidas de protección, de conformidad a la competencia territorial que les asista, deberán: (...) b. Decretar medidas urgentes relativas a material de **texto**, video, audio o imágenes, que serán sometidas a control judicial garantizando los principios de legalidad, necesidad y proporcionalidad y los estándares del derecho internacional de los derechos humanos”.

- **Artículo 11. Medidas de política pública de investigación y sanción**

Sugerimos adicionar al texto la obligatoriedad de formación en género para todos los equipos involucrados en la investigación y sanción de la VG FT. Sin esta capacitación, existe el riesgo de que los agentes encargados de la aplicación de la ley minimicen las denuncias, reproduzcan estereotipos de género o no comprendan el impacto de esta violencia sobre las víctimas/sobrevivientes, lo que puede llevar a impunidad y revictimización[17]. La formación debe incluir las dinámicas específicas de la violencia digital, sus impactos psicológicos y sociales, así como la manera en que el género y la interseccionalidad afectan la experiencia de las víctimas/sobrevivientes.

Además, la capacitación del personal debe incorporar técnicas especializadas para la recolección y preservación de pruebas digitales, asegurando que las investigaciones sean efectivas y respeten los derechos de las víctimas/sobrevivientes. La tecnología evoluciona rápidamente y, sin una actualización constante, los agentes públicos pueden no estar preparados para abordar nuevas formas de violencia digital. La formación continua y

[17] TEDIC (2021). Difusión de imagen no consentida en Paraguay. Online: https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf

obligatoria garantizaría una mayor sensibilidad en la atención a las víctimas/sobrevivientes y precisión en la aplicación de la normativa, fortaleciendo la implementación de la ley y la efectividad de las sanciones contra los responsables.

Sugerencia de redacción: "(...) b. Crear unidades o equipos especializados en violencia digital contra las mujeres por razones de género, dotados de recursos suficientes, **y garantizar la capacitación constante de estos equipos en temas de género, interseccionalidad y tecnologías**;"

- **Artículos 18 y 19**

Los artículos 18 y 19 deben ser revisados para incluir explícitamente los principios de proporcionalidad y debido proceso en la moderación de contenido, lo cual que exige un análisis contextualizado. La moderación de contenido debe realizarse de manera proporcional al daño o riesgo generado, evitando tanto la inacción frente a contenidos violentos como la eliminación excesiva de contenidos que pueda derivar en censura indebida.

Además, la moderación de contenido no debe centrarse únicamente en su eficacia, sino también en los criterios y procesos que la fundamentan. La transparencia sobre los parámetros, reglas y lógicas algorítmicas que rigen la moderación —tanto automatizada como manual— es un requisito indispensable para garantizar que los derechos humanos no se vean comprometidos por decisiones opacas o arbitrarias. Los sistemas de moderación algorítmica suelen operar sin supervisión ni rendición de cuentas, replicando lógicas de poder desiguales y afectando de forma desproporcionada a mujeres y personas de géneros diversos.

En particular, se recomienda precisar en el inciso (ii) del Artículo 18 —referido a las solicitudes gubernamentales de eliminación o restricción de contenido— que estas deben estar sustentadas en una orden judicial previa, emitida por autoridad competente y conforme a las garantías del debido proceso. Esta exigencia resulta clave para evitar abusos de poder, limitar intervenciones arbitrarias y asegurar que toda restricción a la libertad de expresión cumpla con los principios internacionales de legalidad, necesidad y proporcionalidad.

Asimismo, es fundamental que la ley reconozca la importancia del contexto cultural específico de cada país y comunidad en las decisiones sobre moderación de contenido. Por ejemplo, contenidos relacionados con la salud sexual y reproductiva han sido sistemáticamente censurados en diversas plataformas, afectando negativamente el derecho de las mujeres al acceso a la información y a su autonomía corporal. Casos documentados

en Brasil[18] y en Estados Unidos[19] muestran cómo este tipo de censura digital puede vulnerar derechos fundamentales.

Lo que constituye discurso dañino o violencia digital puede variar según factores lingüísticos, políticos y sociales, por lo que es crucial que el equipo responsable de la moderación tenga conocimiento del contexto local y aplique directrices que reflejen esta diversidad para evitar decisiones arbitrarias o sesgadas. Para enfrentar este tipo de sesgos, es indispensable garantizar la supervisión humana en los procesos de moderación, especialmente cuando se trata de expresiones situadas en contextos políticos, culturales o sociales complejos.

Por último, es esencial garantizar que el autor del contenido tenga el derecho de impugnar las decisiones de moderación, con la posibilidad de presentar argumentos y solicitar una revisión. Sin un mecanismo de recurso transparente y accesible, existe el riesgo de que sanciones indebidas restrinjan la libertad de expresión, vulnerando principios democráticos fundamentales. La implementación de procedimientos justos y auditables, con participación significativa de la sociedad civil, fortalecería la credibilidad del proceso, reduciría el riesgo de abusos por parte de plataformas o autoridades, y contribuiría a un ecosistema digital más justo e inclusivo.

- **Artículo 21. Responsabilidad algorítmica**

Es importante reformular el texto para sustituir la expresión "mayor control" por "control total" sobre la experiencia del usuario, de modo que se alinee con los principios de autodeterminación informativa y protección de datos, ampliamente reconocidos en marcos internacionales de derechos digitales y derechos humanos.

El principio de autodeterminación informativa, consagrado en documentos como el Reglamento General de Protección de Datos de la Unión Europea (GDPR) y en legislaciones nacionales de protección de datos, establece que los individuos deben tener control completo sobre sus datos personales, su privacidad y sus interacciones digitales. En el caso de la protección de datos, los estándares internacionales están consagrados en documentos como el UNDP Guide - Drafting Data Protection Legislation, e incluyen principios fundamentales como la transparencia, la limitación del propósito (purpose limitation), la minimización de datos (data minimization) y la rendición de cuentas (accountability).

En este sentido, sugerimos que el artículo 21 incorpore referencias explícitas a estos principios y garantice que las personas usuarias puedan personalizar y restringir su experiencia digital de forma clara, accesible y efectiva, incluyendo mecanismos para otorgar

[18] BRAGA, N. (2019). NET, Claro e Vivo bloqueiam acesso a site com informações sobre aborto seguro. Online: https://www.intercept.com.br/2019/12/12/net-claro-e-vivo-bloqueiam-site-aborto-seguro/

[19] AMNESTY TECH (2024). Obstacles to Autonomy: Post-Roe Removal of Abortion Information Online. Online: https://www.amnestyusa.org/reports/obstacles-to-autonomy-post-roe-removal-of-abortion-information-online/

o retirar consentimiento, gestionar el uso de datos personales y controlar la visibilidad e interacción con los contenidos.

La expresión "mayor control" sugiere una mejora relativa pero aún limitada, mientras que lo ideal sería garantizar un control total, permitiendo que cada usuario decida cómo se recopilan, procesan y utilizan sus datos, así como definir cómo desea interactuar y protegerse en el entorno digital.

Este cambio también refuerza el derecho de las víctimas/sobrevivientes de VG FT a proteger su privacidad y seguridad digital. Muchas formas de VG FT, como *doxxing*, acoso masivo y manipulación algorítmica, ocurren precisamente por la falta de control individual sobre los datos y las configuraciones de privacidad en plataformas digitales. Por lo tanto, la redacción del artículo debería reflejar esta necesidad fundamental de empoderamiento digital pleno, garantizando que las personas usuarias puedan personalizar y restringir su experiencia en línea de manera transparente, accesible y efectiva.

Asimismo, respecto del fragmento “estos algoritmos deberán incorporar la prevención de la violencia digital contra las mujeres por razones de género...”, se recomienda reformular para mayor claridad y evitar ambigüedades que puedan dar lugar a censura o decisiones automatizadas opacas. En lugar de hablar de una "prevención" genérica, se sugiere establecer que los algoritmos deben ser diseñados y auditados con base en criterios de debida diligencia en derechos humanos, incluyendo evaluaciones de impacto con enfoque de género, participación significativa de la sociedad civil y supervisión humana continua.

Sugerencia de redacción: “Los proveedores de servicios que utilicen algoritmos deberán diseñarlos y gestionarlos de manera transparente, ética y accesible en los idiomas locales y con competencia 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 **total control** a las personas usuarias sobre su experiencia digital**, incluyendo la gestión de datos personales, privacidad, visibilidad, contenidos y formas de interacción.**

Los algoritmos deberán ser desarrollados con base en principios de protección de datos y derechos humanos, incluyendo evaluaciones de impacto con perspectiva de género y mecanismos de auditoría periódica. También deberán minimizar la amplificación de contenidos dañinos y mitigar sesgos o estereotipos de género, sin recurrir a mecanismos automatizados de censura, garantizando que toda moderación se base en principios de legalidad, necesidad y proporcionalidad, con supervisión humana.”

- **Artículo 22. Medidas de supervisión de servicios**

El artículo 22 introduce facultades significativas a equipos internos de evaluación de proveedores de servicios digitales, incluyendo la posibilidad de notificar sospechas de delito ante autoridades competentes. Genera preocupaciones significativas que esta notificación

pueda realizarse sin criterios jurídicos claros ni base normativa específica, lo cual genera riesgos considerables de arbitrariedad y criminalización indebida derivada de contenidos o expresiones legítimas. Se recomienda que el texto aclare que **toda notificación de presunto delito debe estar fundamentada en el marco jurídico penal vigente del Estado correspondiente y ser precedida por una verificación mínima de legalidad**, para evitar que empresas actúen como órganos de control penal sin garantías procesales.

Asimismo, la habilitación para suspender servicios o cuentas de manera unilateral, incluso de forma definitiva, plantea riesgos de restricción indebida a la libertad de expresión y a otros derechos fundamentales, especialmente si las decisiones se basan únicamente en el criterio de actores privados. Se sugiere que el artículo incorpore una **referencia expresa al marco internacional de derechos humanos como límite rector, estableciendo que toda medida restrictiva debe respetar los principios de legalidad, necesidad, proporcionalidad y debido proceso**. Esto resulta crucial para evitar usos abusivos de la norma que puedan derivar en censura digital o represalias desproporcionadas, en especial en contextos de alta polarización política o social.

- **Artículo 23. Restricciones a los servicios**

Si bien el artículo 23 establece la obligación de justificar de forma clara y comprensible las restricciones impuestas por los proveedores de servicios, se recomienda complementar esta disposición incorporando la garantía de mecanismos accesibles de apelación. Como ya fue señalado en el comentario al artículo 19, el derecho a impugnar decisiones de moderación o restricción es esencial para evitar arbitrariedades, fortalecer la transparencia y proteger la libertad de expresión. Sin un proceso claro de revisión, las personas usuarias quedan en situación de indefensión frente a decisiones que pueden afectar sus derechos digitales de forma significativa.

Sugerencia de redacción: “Los proveedores de servicios deberán proporcionar a las personas usuarias de sus servicios una declaración de motivos clara y específica cuando se impongan restricciones relacionadas con el uso de sus servicios, incluyendo, pero no limitándose a, la eliminación o bloqueo de contenido, la suspensión o limitación de pagos, la interrupción parcial o total del servicio, o la suspensión o eliminación de cuentas. Estas razones deberán explicarse de manera comprensible y detallada, asegurando que las personas usuarias entiendan las causas detrás de dichas acciones, especialmente en casos donde el contenido proporcionado sea considerado ilegal o incompatible con las condiciones generales del servicio. **Además, deberán garantizar mecanismos accesibles, transparentes y efectivos de apelación para que las personas usuarias puedan impugnar dichas decisiones y solicitar su revisión.** En ningún caso estas restricciones podrán contravenir los derechos garantizados por esta ley ni los principios establecidos en el derecho internacional de los derechos humanos.”

- **Artículo 24. Sistema interno de reclamaciones**

Si bien el artículo 24 establece obligaciones generales para los sistemas internos de reclamaciones, resulta fundamental que el texto incluya una referencia explícita a las

normas comunitarias (como los términos y condiciones o políticas internas de las plataformas), ya que son éstas las que generalmente fundamentan las decisiones de moderación de contenido. Sin esta mención, no queda claro sobre qué base normativa deben ser evaluadas o corregidas dichas decisiones. Además, se recomienda establecer que las normas comunitarias deben respetar los principios del derecho internacional de los derechos humanos y los derechos garantizados por esta ley, a fin de prevenir abusos y censura privada bajo criterios vagos o discriminatorios.

Este resguardo se vuelve aún más urgente frente a la tendencia reciente de las *big techs* a replegar compromisos con los derechos humanos, en respuesta a presiones políticas, económicas o contextos regulatorios cambiantes. Se observa una disminución en la transparencia, desmantelamiento de equipos de derechos humanos y debilitamiento de mecanismos de moderación responsables, en paralelo con el aumento de gobiernos autoritarios que utilizan estas plataformas para difundir desinformación o criminalizar la disidencia. En este escenario, América Latina se encuentra particularmente expuesta, ya que muchas plataformas globales aplican sus reglas de forma opaca y sin adaptarlas a los marcos legales o culturales locales[20]. Por ello, resulta esencial exigir sistemas de reclamo que no solo sean accesibles, sino también fundamentados en principios que limiten la discrecionalidad empresarial y garanticen el debido proceso digital.

Sugerencia de redacción: “Los proveedores de servicios deberán implementar sistemas internos de gestión de reclamaciones que sean accesibles, gratuitos y eficaces, permitiendo a las personas usuarias presentar quejas sobre decisiones relacionadas con la eliminación o restricción de contenido y la suspensión de servicios o cuentas. **Estas decisiones deberán estar debidamente fundamentadas en sus normas comunitarias, las cuales deberán ser accesibles, claras, y conformes con los derechos garantizados por esta ley y con los principios del derecho internacional de los derechos humanos.**
Los mecanismos de reclamación deberán garantizar respuestas oportunas, fundamentadas, no discriminatorias y ajustadas a dichas normas comunitarias y a los principios establecidos en esta Ley.
Cuando una reclamación sea procedente, el proveedor deberá corregir o revertir la medida adoptada sin demora injustificada”

- **Artículo 26. Principios orientadores del proceso**

Se sugiere complementar el artículo 26 con la inclusión explícita de los principios de legalidad, proporcionalidad y razonabilidad, ampliamente reconocidos en el derecho internacional de los derechos humanos como garantías básicas frente a cualquier intervención estatal o restricción de derechos. Estos principios son especialmente relevantes cuando se trata de investigaciones relacionadas con delitos cometidos en entornos digitales, en los que pueden activarse mecanismos de vigilancia, recolección de datos y limitación de acceso a servicios. Tal como se argumentó previamente en este documento (véase comentarios a los artículos 18, 19, 21 y 22), asegurar que toda actuación se ajuste a estos principios es fundamental para prevenir abusos, garantizar la debida

[20] LARA-CASTRO, P. (2025). El rol de las Big Tech en el auge del autoritarismo. Online: https://www.derechosdigitales.org/24797/el-rol-de-las-big-tech-en-el-auge-del-autoritarismo/

protección de los derechos de las víctimas/sobrevivientes y de las personas investigadas, y fortalecer la legitimidad institucional del proceso.

Sugerencia de redacción: “Las investigaciones de los delitos previstos en esta ley deben realizarse siguiendo los siguientes principios rectores: (...) **h. Principios de legalidad, proporcionalidad y razonabilidad**”

- **Artículo 27. Derechos de las víctimas/sobrevivientes en el proceso**

El artículo 27 podría ser fortalecido mediante la incorporación de mecanismos diferenciados que respondan a las múltiples barreras estructurales que enfrentan las mujeres para acceder a la justicia, especialmente en contextos de violencia digital. Desde una perspectiva interseccional, es importante considerar que mujeres indígenas, afrodescendientes, con discapacidad, LBTI, migrantes y privadas de libertad experimentan obstáculos particulares y acumulativos cuando intentan denunciar o participar de procesos judiciales. Por ejemplo, en países como Bolivia, se ha documentado la ausencia de intérpretes en lenguas indígenas y la falta de atención jurídica con enfoque cultural, lo que limita gravemente la comprensión del proceso y la posibilidad de defensa efectiva[21].

Asimismo, se recomienda que el artículo reconozca la necesidad de establecer múltiples vías de acceso a la justicia, incluyendo mecanismos presenciales, móviles y digitales, capaces de adaptarse a las realidades geográficas, económicas y socioculturales de las víctimas/sobrevivientes. La centralización de los servicios judiciales en zonas urbanas excluye a mujeres que viven en áreas rurales o periurbanas, quienes a menudo carecen de conectividad, transporte o información adecuada.

Finalmente, se sugiere reforzar el artículo incorporando garantías claras de participación activa, informada y segura de las mujeres en el proceso, asegurando que su voz no sea meramente testimonial, sino que tenga impacto real en las decisiones judiciales. Esto implica también adoptar medidas para prevenir la revictimización, reconocer los riesgos de represalias digitales y asegurar entornos de acompañamiento adecuados. Muchas mujeres desisten de continuar los procesos debido a la falta de seguimiento institucional, a la exposición pública en redes sociales o a la ausencia de medidas de protección adecuadas para ellas y sus familias[22].

Sugerencia de redacción: “El Ministerio o Secretaría de Justicia, en coordinación con el Ministerio Público y los mecanismos nacionales competentes, deberán garantizar a las mujeres víctimas y sobrevivientes y a sus familiares, los siguientes derechos, a través de la creación de directrices específicas: (...)

[21] DERECHOS DIGITALES; TEDIC; HIPERDERECHO; FUNDACIÓN INTERNETBOLIVIA.ORG (2025). Contribución a la consulta de la Comisión Interamericana de Derechos Humanos de la OEA sobre Acceso de las mujeres a la justicia en casos de violencia y discriminación: estudio de situación en las Américas y el Caribe. Online:https://www.derechosdigitales.org/wp-content/uploads/cciddhh.pdf
[22] Ibid

f. Acceso a múltiples vías de justicia, incluyendo canales presenciales, móviles y digitales accesibles en zonas rurales y comunidades marginadas;
g. Participación segura y sin represalias en los procesos judiciales, con acompañamiento institucional efectivo y medidas de protección adecuadas;
h. Garantía de enfoque interseccional en todas las etapas del proceso, considerando la situación específica de mujeres indígenas, afrodescendientes, LBTI, con discapacidad, migrantes y privadas de libertad."

- **Adición al Capítulo III. Rendición de cuentas**

Debe añadirse al Capítulo III, que regula a las empresas, una disposición específica que obligue a los proveedores de servicios digitales a realizar evaluaciones de impacto en derechos humanos con enfoque de género, antes de lanzar sus productos o servicios al mercado o antes de modificar el funcionamiento de productos o servicios ya existentes. Estas evaluaciones constituirían una medida precautoria esencial, garantizando que las herramientas tecnológicas, plataformas digitales y sistemas automatizados no reproduzcan ni amplifiquen desigualdades de género ni faciliten formas de VG FT.

Estas evaluaciones de impacto en derechos humanos con perspectiva de género deberían realizarse antes del lanzamiento del servicio y revisarse periódicamente para identificar riesgos y corregir fallas que puedan derivar en discriminación, vigilancia desproporcionada, acoso o violencia digital contra mujeres y personas LGBTQIA+. La obligación de llevarlas a cabo representaría una de las principales medidas de rendición de cuentas de las empresas ante la sociedad, exigiendo que demuestren transparencia, compromiso con la no discriminación y mecanismos eficaces de mitigación de riesgos.

Esta práctica ya ha sido debatida en regulaciones internacionales, como la Ley de Servicios Digitales de la Unión Europea (Digital Services Act - DSA), que impone obligaciones a las plataformas de gran alcance para que realicen evaluaciones de riesgo sistémico, incluyendo impactos sobre los derechos fundamentales y la seguridad de las usuarias.

Por lo tanto, incluir esta exigencia en la Ley Modelo Interamericana garantizaría un marco regulatorio sólido para prevenir violaciones de derechos humanos y proteger a los grupos históricamente marginados en el entorno digital. Esta obligación también se alinea con los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas, particularmente con el Principio 18, que establece que las empresas deben identificar y evaluar los impactos negativos reales y potenciales sobre los derechos humanos, prestando atención especial a los riesgos para los grupos o poblaciones vulnerables o marginadas.

- **Artículo 28. Legitimación procesal**

Sugerimos incluir en el Artículo 28 una disposición que fomente la implementación de mecanismos accesibles para la presentación de denuncias, como la posibilidad de registro en línea, garantizando que las víctimas/sobrevivientes y terceros puedan reportar

casos de VG FT de manera segura y accesible. Dado que este tipo de violencia ocurre mayoritariamente en entornos digitales, es fundamental que las víctimas/sobrevivientes tengan canales de denuncia igualmente digitales, sin la necesidad de acudir presencialmente a una comisaría u otra autoridad competente, lo que puede representar un obstáculo significativo, especialmente para mujeres en situación de vulnerabilidad.

Además, la denuncia en línea podría permitir la presentación de pruebas digitales, como capturas de pantalla, enlaces y metadatos, facilitando la investigación y recolección de evidencia. Garantizar mecanismos de denuncia accesibles y no burocráticos contribuiría a la efectividad de la ley y mejoraría el acceso a la justicia para las víctimas/sobrevivientes de VG FT.

En ese sentido, se recomienda también que la ley establezca criterios mínimos para asegurar el resguardo de los datos personales y de las evidencias aportadas en el proceso de denuncia digital, garantizando su confidencialidad, integridad y uso exclusivo para fines judiciales. Estos mecanismos deben diseñarse en conformidad con los estándares internacionales de derechos humanos, incluyendo principios como la seguridad de la información, la cadena de custodia digital y la no revictimización.

Sugerencia de redacción: “La denuncia podrá ser presentada por la víctima o víctimas o sobrevivientes, por terceros o cualquier persona natural o jurídica, **a través de mecanismos accesibles y simplificados**, siempre que se esté frente a un posible delito de violencia digital contra las mujeres por razones de género de acción pública, y en casos de delitos de violencia digital contra las mujeres por razones de género de acción privada, cuando lo autorice la víctima.”

- **Artículos 33 y 34**

Los artículos 33 y 34 establecen que todas las conductas de VG FT previstas en el artículo 7 sean tratadas como delitos de acción pública y sujetas a penas de privación de libertad. Sin embargo, es importante cuestionar si todas las conductas listadas deben necesariamente criminalizarse y si, en todos los casos, la sanción debe ser restricción de la libertad. La criminalización puede ser una herramienta importante para disuadir y sancionar actos graves de violencia digital, pero no siempre es la respuesta más efectiva ni proporcional[23]. Además, tal como dijimos en los comentarios al artículo 8e, la ley penal con frecuencia es aplicada de manera arbitraria y contraria a grupos vulnerables.

Un aspecto preocupante es la gran variabilidad en la gravedad de las conductas descritas en los artículos. Por ejemplo, hay una diferencia significativa entre "inducir, coaccionar o facilitar el suicidio de una mujer mediante el uso de tecnologías" e "implementar o utilizar inteligencia artificial o sistemas automatizados que generen discriminación de género". La primera es una conducta extremadamente grave, con consecuencias irreversibles para la víctima/sobrevivientes, que podría justificar una respuesta penal. En cambio, la segunda, aunque problemática y generadora de

[23] Hiperderecho. (2021). Después de la Ley: Informe Nro 3. https://hiperderecho.org/wp-content/uploads/2021/08/Informe-3_Despues-de-la-ley.pdf

desigualdades estructurales, podría abordarse mejor mediante mecanismos administrativos o regulatorios, como sanciones económicas a las empresas responsables y la obligación de revisar algoritmos y sistemas de toma de decisiones automatizados.

Además, una criminalización excesiva puede generar desafíos prácticos. Muchos países de América Latina tienen sistemas de justicia penal sobrecargados e ineficientes, lo que dificulta la aplicación de penas privativas de libertad para delitos que podrían ser mejor abordados mediante vías administrativas o civiles. Asimismo, en algunos contextos, el derecho penal ha sido históricamente utilizado de manera selectiva, sin necesariamente responder a las necesidades de las víctimas/sobrevivientes, quienes muchas veces buscan reparación, protección y la interrupción del daño, más que la punición del agresor.

Este punto se ve reflejado en estudios recientes. Por ejemplo, en Paraguay, investigaciones de TEDIC sobre la difusión no consentida de imágenes íntimas revelaron que muchas víctimas/sobrevivientes optan por no acudir a la vía penal, ya que no responde a lo que realmente necesitan, como el retiro del contenido, apoyo psicológico o protección frente a represalias[24].

En este sentido, es fundamental adoptar un enfoque centrado en la víctima/sobreviviente, que priorice sus derechos, necesidades y seguridad por sobre una lógica exclusivamente punitiva. Un marco legal centrado en las víctimas/sobrevivientes permitiría articular respuestas más eficaces, incluyendo mecanismos de reparación, apoyo psicosocial, medidas cautelares y protección efectiva, así como caminos alternativos a la justicia penal, como vías administrativas, civiles o constitucionales.

La experiencia también muestra que los abordajes exclusivamente penales no solo han sido ineficientes, sino que, en algunos casos, han puesto a las víctimas/sobrevivientes en mayor riesgo. El informe conjunto de Derechos Digitales y APC documenta cómo las leyes de cibercrimen han sido utilizadas para criminalizar a mujeres y personas LGBTQIA+ en al menos once países, incluyendo casos en los que víctimas/sobrevivientes de violencia digital fueron procesadas por difamación tras denunciar públicamente los abusos sufridos[25].

Por ello, sería recomendable que la ley modelo diferenciara mejor la gravedad de las conductas y considerara sanciones alternativas, como multas, suspensión de actividades u otras medidas más proporcionales y efectivas en ciertos casos. La CSW67, en sus conclusiones, también recomendó estrategias legislativas multifacéticas para abordar la VG FT, que incluyan no solo la penalización, sino también reformas administrativas, regulatorias y educativas, siempre desde un enfoque de derechos y centrado en las víctimas/sobrevivientes[26].

---

[24] TEDIC (2021). Difusión de imagen no consentida en Paraguay. Online: https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf
[25] DERECHOS DIGITALES; APC (2023). Online: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf
[26] CSW67 Agreed conclusions (2023). Online: https://www.unwomen.org/sites/default/files/2023-03/CSW67_Agreed%20Conclusions_Advance%20Unedited%20Version_20%20March%202023.pdf

- **Artículos 39 y 40**

Los artículos 39 y 40 del documento establecen la creación de una Autoridad Nacional Administrativa con competencia para sancionar a los proveedores de servicios que infrinjan las disposiciones de la ley. Para que esta autoridad sea efectiva y garantice la protección de las víctimas/sobrevivientes de VG FT, es fundamental que sea independiente y cuente con recursos humanos y financieros suficientes. Sin esta estructura, existe el riesgo de que sus funciones sean meramente simbólicas, sin capacidad real para supervisar, aplicar sanciones y garantizar la implementación efectiva de la ley. Además, la falta de independencia podría dar lugar a captura política o corporativa, lo que comprometería su imparcialidad en la aplicación de la normativa.

No obstante, es importante considerar si la creación de una autoridad con este nivel de autonomía y estructura es realista para todos los países de las Américas. Muchas naciones de la región aún no cuentan con organismos reguladores específicos para temas tecnológicos, lo que genera dudas sobre la viabilidad de establecer una entidad con atribuciones tan amplias. Por ejemplo, países como Paraguay y Bolivia no disponen de una agencia especializada en regulación digital y protección de datos. Además, en algunos países, la falta de presupuesto y de prioridad política en la lucha contra la VG FT podría dificultar la implementación de una autoridad con independencia y estructura adecuadas.

Ante esta realidad, sería prudente que la ley modelo reconociera la diversidad institucional de la región y ofreciera alternativas para la implementación de esta autoridad, permitiendo que los países ajusten sus estructuras según su contexto. Una posible solución sería asignar estas funciones a organismos ya existentes, como agencias de protección al consumidor o mecanismos nacionales de derechos humanos, siempre que cuenten con mandatos claros y sean fortalecidos con recursos y capacitación para abordar casos de VG FT. De esta manera, la regulación sería más viable y adaptable a la realidad institucional de cada país, sin comprometer la protección de las víctimas/sobrevivientes.

- **Artículo 42. Destinación de recursos provenientes de las sanciones económicas**

Sería recomendable ampliar el artículo sobre la asignación de los recursos obtenidos a través de sanciones económicas en casos de violencia digital contra las mujeres por razones de género, incluyendo la posibilidad de que estos fondos también puedan financiar iniciativas de la sociedad civil y comunitarias que trabajen comprobablemente en la prevención de la VG FT o en la asistencia directa a las víctimas/sobrevivientes. Esta ampliación garantizaría que los recursos no solo fortalezcan la respuesta institucional del Estado, sino que también apoyen a organizaciones especializadas que ya desempeñan un papel crucial en la lucha contra la VG FT.

Un referente útil para esta propuesta es el Fondo de Derechos Difusos (FDD) de Brasil, que utiliza los valores provenientes de condenas en acciones civiles públicas para financiar proyectos de interés colectivo. En el caso del FDD, los recursos se destinan a iniciativas para la protección del medio ambiente, los derechos del consumidor y otros derechos fundamentales, según criterios definidos por un consejo gestor. Este modelo

podría adaptarse para garantizar que las organizaciones que brindan asistencia a víctimas/sobrevivientes de VG FT o trabajan en su prevención puedan acceder a estos fondos, siempre que cumplan con requisitos de transparencia y demuestren impacto en su labor.

En América Latina, existen diversas iniciativas comunitarias clave para apoyar a las víctimas/sobrevivientes de VG FT, como lo demuestra la investigación de Derechos Digitales sobre algunas líneas de ayuda disponibles en la región[27]. Estas líneas ofrecen atención psicológica, orientación jurídica y soporte técnico a las víctimas/sobrevivientes de violencia digital, muchas veces cubriendo vacíos que dejan las respuestas estatales. Incluir la posibilidad de destinar parte de los recursos obtenidos por sanciones económicas para fortalecer estas iniciativas garantizaría mayor alcance y capilaridad en la protección de las víctimas/sobrevivientes, asegurando que la respuesta al VG FT sea más efectiva y descentralizada.

- **Artículo 43. Responsabilidad civil de los proveedores de servicios**

Sugerimos mantener la disposición del Artículo 43 sobre responsabilidad civil, pero incluir expresamente el derecho de la víctima/sobreviviente a optar exclusivamente por la vía civil de reparación, sin la necesidad de iniciar una acción penal. Como ya se ha señalado anteriormente, la criminalización no siempre es suficiente ni necesariamente deseada por las víctimas/sobrevivientes, quienes muchas veces no encuentran en el sistema penal un camino adecuado para su reparación. Algunas víctimas/sobrevivientes pueden temer represalias, desconfiar de las instituciones de justicia penal o simplemente preferir una respuesta más rápida y menos desgastante emocionalmente que un proceso penal[28].

Además, en muchos casos, la responsabilidad civil puede ser más efectiva para reparar los daños, permitiendo indemnizaciones y medidas compensatorias sin la necesidad de probar un delito penal. Por lo tanto, para garantizar mayor autonomía y acceso a la justicia, el texto del artículo debería asegurar que la víctima/sobreviviente tenga el derecho de buscar reparación civil, independientemente del resultado o de la existencia de un proceso penal.

---

[27] DERECHOS DIGITALES (2024). Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador. Online: https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ESP.pdf

[28] Hiperderecho. (2021). Después de la Ley: Informe Nro 3. https://hiperderecho.org/wp-content/uploads/2021/08/Informe-3_Despues-de-la-ley.pdf