

Ley Modelo de Violencia Digital contra las mujeres por razones de género

Comentarios Unidad Especializada en Delitos Sexuales y de Explotación Sexual (UDSEX), Fiscalía Nacional, Ministerio Público de Chile

Santiago, 07 de abril de 2025

La atención de la UDSEX en la iniciativa se debe al impacto que cualquier modificación en la materia puede significar en la persecución penal de estas conductas y, en consecuencia, en el correcto acceso a justicia y protección de las víctimas de estos delitos, especialmente cuando se trata de mujeres y niñas y cuando las conductas afectan de algún modo su integridad, libertad o indemnidad sexual.

I. Observaciones generales a la iniciativa

De acuerdo con los datos levantados por la Unidad de Género y Participación Ciudadana de la Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública de Chile en su Consulta Ciudadana Virtual sobre Violencia Digital el año 2023¹, en el país el grupo de personas más expuestas a sufrir violencia digital corresponde a niñas, niños y adolescentes (88%) y mujeres (65%), siendo las formas más recurrentes de violencia digital la violencia a través de mensajes escritos o audios (66%), hostigamiento y/o acoso (47%), y difamación (45%). Otros estudios han indicado que 7 de cada 10 adolescentes mujeres ha vivido alguna manifestación de violencia en internet².

En ese sentido, al momento de analizar y adoptar medidas legislativas, es necesario comprender que la violencia digital en contra de mujeres de todas las edades es una manifestación del fenómeno estructural de la violencia de género, situándose dentro de patrones sociales más amplios de poder y desigualdad que ya existían antes de la llegada del Internet, y que ahora se han entrelazado e interactuado con las nuevas tecnologías³. Teniendo presente lo anterior, valoramos la propuesta pues las conductas que busca sancionar no se encuentran debidamente abordadas en el Código Penal chileno, a pesar de constituir hechos que afectan de forma relevante la privacidad, seguridad, integridad psíquica, honor, dignidad y la propia imagen de las víctimas⁴.

En este contexto, es relevante resaltar los esfuerzos realizados en los últimos años por el Mecanismo de Seguimiento de la Convención Belem do Pará (MESECVI) y ONU Mujeres. Es fundamental considerar las definiciones y tipologías de violencia digital presentes en la Ley Modelo, donde se reconocen tipos de violencia como el ciberhostigamiento, el ciberacoso, la creación, difusión, publicación, distribución, intercambio, manipulación y almacenamiento de registros de naturaleza sexual, el acceso no consentido y/o ataque a la integridad de sistemas informáticos, la suplantación y robo de identidad en línea, actos de monitoreo, control y vigilancia, ataques a la reputación o credibilidad de la víctima, entre otros.

¹ Disponible en: <https://generoyparticipacion.interior.gob.cl/media/2023/12/Resultados-Consulta-Ciudadana-Virtual-sobre-Violencia-Digital.pdf>

² ONU Mujeres Chile (2020). Violencia digital: Experiencias virtuales de niñas y adolescentes en Chile. Disponible en: <https://datosprotegidos.org/descarga-resultados-encuesta-violencia-digital-experiencias-virtuales-de-ninas-y-adolescentes-en-chile/>

³ Ibid.

⁴ Fundación Datos Protegidos (2018). Violencia de género en internet en Chile, p.4. Disponible en: <https://datosprotegidos.org/wp-content/uploads/2018/12/Informe-Violencia-de-ge%CC%81nero-en-Internet-en-Chile.pdf>

A continuación, se presentan algunas observaciones que se estiman pertinentes de considerar al momento de legislar en la materia:

1. Violencia digital contra niños y adolescentes varones

Si bien la Ley Modelo se centra, con justa razón, en la violencia digital contra mujeres por razones de género, consideramos importante señalar que ciertas manifestaciones de esta violencia también pueden afectar a niños y adolescentes varones, especialmente cuando se vinculan con estereotipos de género o castigos sociales ante expresiones no normativas de la masculinidad. La experiencia investigativa muestra que los varones adolescentes pueden ser objeto de humillaciones públicas, exposición no consentida de imágenes íntimas u hostigamientos digitales por razones vinculadas a su orientación sexual o identidad de género, configurando formas de violencia que también se entrelazan con estructuras de desigualdad. Una legislación comprehensiva debiese tener presente esta realidad, particularmente en el diseño de estrategias preventivas, de persecución penal y de reparación.

2. Violencia digital cometida por adolescentes

Es esencial considerar que diferentes manifestaciones de violencia digital que comprende esta Ley Modelo afectarán especialmente a las/os adolescentes, quienes son un grupo etario activo en el espacio digital. En este sentido, las/os adolescentes podrán verse mayormente involucrados como autoras/es de este tipo de conductas, ya sea actuando individualmente o bien en grupos, lo que puede traer aparejado un alza en su criminalización.

La eventual criminalización de adolescentes como responsables de manifestaciones de violencia digital exige reconocer su especial condición y, por tanto, imponer un tratamiento diferenciado respecto del sistema penal de personas adultas. En este sentido, la persecución penal de adolescentes debe guiarse por los principios de especialización, mínima intervención, proporcionalidad, justicia restaurativa y protección integral de derechos, procurando respuestas que privilegien la educación, la reflexión crítica y la reparación por sobre la sanción punitiva. El establecimiento de tipos penales amplios, circunstancias agravantes o la previsión de penas privativas de libertad de carácter generalizado podría contravenir estos principios y afectar desproporcionadamente a esta población, por lo que resulta indispensable una regulación acorde a los estándares internacionales en materia de justicia juvenil.

3. Determinación de la competencia

Si bien el proyecto de Ley Modelo contempla un apartado relativo a la jurisdicción de los Estados sobre los delitos, lo cierto es que ante este tipo de delitos surge una dificultad adicional relativa a la determinación del tribunal competente para conocer estas conductas pues muchas de éstas se cometen a distancia, encontrándose víctima e imputado en ciudades o incluso países distintos.

Cabe indicar que las reglas de competencia establecidas en el Código Orgánico de Tribunales de Chile no fueron diseñadas para delitos cometidos por medios digitales, sino que para ilícitos ejecutados en el mundo físico⁵. De esta manera, es común que jueces/zas discutan su competencia para conocer estos hechos, atendiendo

⁵ Puede consultarse Biblioteca del Congreso Nacional de Chile (2015). Delitos Informáticos. Chile y legislación extranjera, pp. 22 y 40. Disponible en: <https://www.camara.cl/verDoc.aspx?prmTIPO=DOCUMENTO COMUNICACIONCUENTA&prmID= 11020>

comúnmente a criterios geográficos que no son útiles en estos casos (por ejemplo, el domicilio de la persona imputada, siendo que puede haber ejecutado la acción en cualquier lugar a través de su celular). Todo esto retrasa las investigaciones y también puede afectar a las víctimas, al definirse que el tribunal competente es uno distinto al de su domicilio (incluso en otra región).

De esta manera, una adecuada regulación de la violencia digital debe considerar la creación de una regla especial de competencia (para los delitos que se pretenden crear y para toda otra conducta que pueda cometerse mediante Internet). Una posible solución es el establecimiento de una especie de *jurisdicción universal* para conocer de los hechos delictivos cometidos mediante tecnologías, independientemente del lugar donde se encuentre quien los comete. Por otra parte, también puede adoptarse una regla basada en la *teoría de la ubicuidad*, que ha tenido acogida en la jurisprudencia española y nacional, según la cual será competente un tribunal cuando alguno de los elementos centrales del hecho (los actos ejecutivos de la comisión del delito, el resultado dañoso de la conducta, el beneficio o lucro de los/as autores/as, etc.) se cometa en su territorio⁶.

4. Capacidades investigativas

Finalmente, se valora especialmente lo señalado en el artículo 12 letra b) en cuanto a establecer como deber del Estado la conformación de unidades o equipos especializados en violencia digital contra las mujeres por razones de género y que estén dotadas de recursos suficiente. La investigación de delitos de violencia digital demanda una mayor especialización y de recursos materiales/tecnológicos en comparación con otros tipos de delitos. Actualmente, la situación en Chile es crítica pues las unidades especializadas operan al límite de su capacidad debido al alto volumen de casos relacionados con delitos vigentes, lo que resulta en demoras significativas.

II. Observaciones al articulado propuesto

Considerando que el Ministerio Público de Chile únicamente tiene facultades constitucionales para investigar delitos, ejercer la acción penal y dar protección a víctimas y testigos, a continuación, se indican algunos comentarios respecto a las disposiciones que dicen relación con tal ámbito de competencias:

1. Artículo 5. Definiciones

Resulta llamativa la amplitud del concepto de proveedores de servicios, particularmente respecto del alcance estipulado en el numeral iii) respecto a entidades públicas o privadas que *comercialicen* productos tecnológicos que permitan la captura, almacenamiento, procesamiento o transferencia de datos electrónicos y datos personales.

Lo anterior resulta especialmente complejo cuando se vincula con lo dispuesto en los artículos 18 y siguientes que establecen ciertas obligaciones de comunicación a las autoridades, moderación de contenido y responsabilidad algorítmica, entre otros. La

⁶ Ver, por ejemplo, Flores Prada, Ignacio (2015). "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", en *Revista Electrónica de Ciencia Penal y Criminología* (en línea), núm. 17-21, pp. 1-40, p. 31. Disponible en: <http://criminet.ugr.es/recpc/17/recpc17-21.pdf>

extensión del concepto hacia entidades que únicamente cumplan el rol de comercialización puede resultar ajena a los fines buscados por la ley modelo.

En este sentido, se sugiere delimitar con mayor precisión el concepto de proveedor de servicios, circunscribiéndolo a quienes efectivamente administren, gestionen o tengan injerencia directa en el funcionamiento de plataformas digitales o en el tratamiento de datos personales, con el fin de evitar regulaciones desproporcionadas o de difícil exigibilidad.

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

Se valora positivamente la incorporación de un catálogo amplio y detallado de conductas que configuran manifestaciones de violencia digital por razones de género, muchas de las cuales no se encuentran suficientemente reconocidas en la legislación penal chilena vigente. Esta enumeración permite visibilizar prácticas que afectan gravemente derechos fundamentales como la privacidad, la integridad psíquica, el honor y la dignidad de las mujeres.

Con todo, se estima pertinente formular una observación respecto de la **letra m)**, que alude a la implementación, diseño o uso de algoritmos o herramientas digitales que generen sesgos discriminatorios, favorezcan la difusión de contenido violento explícito contra mujeres, o promuevan la violencia en su contra. La amplitud de los verbos rectores utilizados en esta disposición —como “favorezcan” o “promuevan”— podría dar lugar a interpretaciones extensivas o indeterminadas sobre la conducta sancionada, afectando principios como el de legalidad penal y de tipicidad.

Por ello, se sugiere considerar la inclusión de una cláusula que exija un elemento subjetivo específico, como un conocimiento previo o intención deliberada (a sabiendas, maliciosamente u otro equivalente), que permita acotar la aplicación de esta norma a supuestos en que efectivamente exista una conducta dolosa y con ánimo discriminatorio.

3. Artículo 10 bis. Medidas de protección de urgencia

Dentro de estas medidas se contempla de Comisarías de Familia, tribunales de control de garantía u otros órganos judiciales y administrativos competentes pueda decretar medidas urgentes relativas al material de video, audio o imagen.

No obstante, considerando la volatilidad, fragilidad y alta replicabilidad del contenido digital, así como su relevancia probatoria en los procesos penales, se estima necesario establecer expresamente que la adopción de estas medidas no podrá implicar la destrucción del material sin que se haya garantizado previamente su respaldo y conservación.

La ausencia de una obligación clara en este sentido podría generar situaciones en las que el retiro del contenido por razones de protección implique la pérdida de evidencia clave para la persecución penal de los hechos, afectando tanto el deber del Estado de investigar como los derechos de las víctimas a obtener verdad y justicia.

En consecuencia, se sugiere incorporar una disposición que exija la preservación del contenido digital retirado, junto con sus metadatos y demás elementos técnicos, en

condiciones que aseguren su integridad, autenticidad y disponibilidad para fines investigativos.

4. Artículo 14. Responsabilidad de las personas funcionarias públicas

Al respecto, y analizada en conjunto con lo dispuesto en el artículo 29 (tipo de acción penal), surgen dudas respecto de dos elementos:

- El carácter de la acción penal cuando se trate de personas funcionarias públicas y el qué se entenderá por estar “legamente obligados a actuar”.
- Asimismo, cuáles serán los alcances del “conocimiento de delitos de violencia digital”, habida cuenta que las características propias de este tipo de manifestaciones que ocurren en el internet, teniendo un amplio alcance y que puede difundirse masivamente, de manera que simultáneamente diversos/as funcionarios/as públicos/as tomen conocimiento. Lo anterior puede repercutir en duplicidades de denuncias y procedimientos que pueden significar una victimización secundaria hacia las mujeres.

5. Artículos 18 y 19. Notificación de sospechas de violencia contra las mujeres y niñas; Moderación de contenidos.

Los artículos 18 y 19 abordan mecanismos de notificación y moderación de contenidos por parte de los proveedores de servicios digitales, en caso de indicios razonables de violencia digital contra mujeres y niñas. Sin perjuicio del objetivo legítimo de proteger a las víctimas y detener la circulación de contenidos violentos, se estima necesario formular algunas reservas respecto del alcance y aplicación de estas normas.

En primer lugar, la habilitación a los proveedores de servicios para revisar contenido (ya sea de forma manual o mediante herramientas automatizadas) ante la mera existencia de “indicios razonables” podría entrar en tensión con garantías fundamentales, particularmente el derecho a la privacidad de las comunicaciones y el principio de legalidad en la obtención de evidencia. En efecto, la intervención o revisión de contenido sin autorización judicial puede comprometer la licitud de los medios de prueba, afectando la validez del procedimiento penal.

Asimismo, el umbral de “indicios razonables” resulta jurídicamente difuso, especialmente cuando se delega su apreciación a actores privados que no cuentan con criterios uniformes ni control jurisdiccional previo. Esto puede generar decisiones arbitrarias o dispares respecto a qué contenido se considera violento o perjudicial, con consecuencias importantes tanto para la libertad de expresión como para la eficacia de las investigaciones.

6. Artículo 20. Mecanismos internos de denuncia

Tal como se indicó previamente en relación con el artículo 10 bis, se debería especificar expresamente que la solicitud de eliminación, suspensión o restricción realizada a los proveedores de servicios tenga aparejada una obligación de preservar dicho contenido, así como todo otro dato informático e información del usuario vinculado, por si fuere solicitado por el organismo investigativo correspondiente.

En la práctica, el retiro inmediato de contenido sin respaldo puede generar la pérdida irrecuperable de pruebas esenciales, afectando tanto el deber del Estado de investigar como los derechos de las víctimas a obtener justicia.

7. Artículo 23. Medidas de suspensión de servicios

Si bien dicha medida puede ser efectiva para frenar la continuidad del daño, se identifican dos aspectos que conviene revisar con mayor detención.

En primer lugar, al igual que en los artículos anteriores, se estima indispensable que la adopción de cualquier medida de suspensión vaya acompañada de la obligación expresa de preservar y respaldar todos los datos informáticos asociados, incluyendo contenido, tráfico, registros de conexión y metadatos del usuario afectado. De no contemplarse esta exigencia, existe el riesgo de pérdida de información relevante para una eventual investigación penal, obstaculizando la identificación de responsables y la obtención de justicia para la víctima.

En segundo lugar, la medida de suspensión establecida en el supuesto del inciso segundo, esto es, existencia de conductas reiteradas, puede ser contraria a algunas regulaciones internacionales en materia de material de abuso o explotación sexual de niñas, niños y adolescentes, las que mandatan el cierre inmediato de la cuenta.

8. Artículo 29. Legitimación procesal

El artículo 29 regula la legitimación activa para ejercer acciones en el marco de los delitos previstos por la Ley Modelo. No obstante, al ser analizado conjuntamente con otras normas, por ejemplo, su artículo 14 —referido a la responsabilidad de personas funcionarias públicas— surgen interrogantes relevantes respecto de la naturaleza de la acción penal aplicable y su impacto en los derechos de las víctimas.

En particular, no queda claro qué criterios se utilizarán para distinguir entre delitos de acción pública y delitos de acción privada, ni cómo se garantizará la debida protección de la intimidad de las mujeres víctimas en cada caso.

9. Artículo 30. Medidas cautelares

En relación con la delimitación del momento en que debe resolverse la imposición de alguna medida cautelar, se sugiere modificar la expresión utilizada a fin de contemplar escenarios en los cuales se puedan decretar de manera previa a la imputación.

En el sistema procesal penal chileno, existen medidas cautelares que pueden ser decretadas antes de la formalización de la investigación, lo que permite una respuesta temprana del sistema frente a situaciones de riesgo o urgencia. Limitar las medidas cautelares únicamente a etapas posteriores podría dejar desprotegidas a las víctimas en la fase inicial de la investigación, que muchas veces es la más crítica.

10. Artículos 35 y 37. Penas y circunstancias agravantes

El artículo 35 establece que las conductas descritas en la Ley Modelo serán sancionadas con penas privativas de libertad, mientras que el artículo 37 contempla como circunstancia agravante que los hechos sean cometidos por dos o más personas conjuntamente. Si bien estas disposiciones responden a la gravedad de los efectos que la violencia digital puede generar sobre las víctimas, es necesario realizar algunas observaciones desde la perspectiva de la justicia penal adolescente.

Tal como se señaló anteriormente, las/os adolescentes constituyen un grupo altamente activo en entornos digitales, tanto en calidad de potenciales víctimas como de posibles

autoras/es de conductas sancionables. La tipificación amplia de ciertos comportamientos —unida a la previsión general de penas privativas de libertad y la agravación por actuar en grupo— puede tener como efecto una criminalización desproporcionada de adolescentes, especialmente en contextos de interacción grupal como redes sociales, videojuegos o entornos escolares virtuales.

Estas previsiones podrían entrar en tensión con los principios que rigen el sistema de responsabilidad penal adolescente, particularmente los de especialización, justicia restaurativa, mínima intervención y proporcionalidad, reconocidos tanto en la legislación nacional como en los estándares internacionales de derechos humanos.