CELE
Centro de Estudios en Libertad de Expresión

Documento de posición

25

Comentarios al proyecto de Ley Modelo Interamericana para prevenir, sancionar y erradicar la violencia digital contra las mujeres por razones de género

CELE

8 de abril de 2025

CELE, Comentarios al proyecto de Ley Modelo Interamericana para prevenir, sancionar y erradicar la violencia digital contra las mujeres por razones de género, Documento de posición No. 25 (ESP), Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2025)

UP
Universidad de Palermo

Facultad de Derecho

Centro de Estudios en Libertad de Expresión

Comentarios al proyecto de Ley Modelo Interamericana para prevenir, sancionar y erradicar la violencia digital contra las mujeres por razones de género

Buenos Aires, Argentina, 8 de abril de 2025

Respetado Comité de Expertas de MESECVI

Organización de Estados Americanos

Asunto: Consulta Ley Modelo de Violencia Digital

De nuestra mayor consideración,

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo fue creado con el objetivo de proveer investigaciones de carácter académicas a periodistas, instituciones gubernamentales, unidades académicas y demás sectores de la sociedad civil dedicados a la defensa y a la promoción de estos derechos. El trabajo del CELE responde a la necesidad de constituir espacios abiertos al debate dedicados a estos temas de interés como en la presente diligencia.

Desde el CELE queremos expresar nuestro profundo interés por el proyecto de ley modelo de violencia digital desarrollado por el comité de expertas, y por tanto, hacemos llegar la presente contribución que pretende aportar en el fortalecimiento de la protección del derecho a la libertad de expresión en el contexto de prevención, protección y atención de la violencia de género digital. Esta contribución se concentrará en dos puntos: (a) la importancia de resguardar el principio de legalidad a la hora de diseñar acciones o políticas públicas que afecten a la libertad de expresión; y (b) el marco general de la responsabilidad de los intermediarios, que es afectado por aspectos claves de este proyecto.

Principio de legalidad y restricciones a la libertad de expresión

La violencia en línea contra las mujeres es un fenómeno que causa creciente preocupación, y constituye—en sí mismo—uno de los mecanismos a través de los cuales se afecta la libre participación de las mujeres en el debate público. La violencia de género digital no es un fenómeno autónomo o aislado: tiene efectos y consecuencias en los espacios físicos y en la violencia que se genera en estos en razón del género y como resultado de relaciones de poder que perpetúan la desigualdad de las mujeres. Consideramos que la ley modelo representa un avance en este sentido, en particular en tanto la norma propone una aproximación abarcativa de la problemática. Pero—a la vez—consideramos que debe modificarse en algunos aspectos, para que ésta sea plenamente compatible con la Convención Americana de Derechos Humanos y los estándares interamericanos en materia de libertad de expresión. En efecto, las respuestas de los estados a este problema deben ser proporcionadas, respetar los estándares de derechos humanos en materia de restricciones legítimas a la libertad de expresión, y deben estar diseñadas de manera acotada para prevenir que su abuso con fines de censura directa o indirecta.

El punto de *tensión* más fuerte que encontramos entre la ley modelo y esos estándares se relaciona con el *principio de legalidad* que constituye el primer paso de análisis del *test tripartito* interamericano[1]. Este principio exige precisión en el lenguaje en el que se redactan restricciones a la libertad de expresión o medidas que impactan o afectan ese derecho. Por ello, es imprescindible que los legisladores de los países miembros precisen conceptos, eviten ambigüedades y cláusulas abiertas, y dispongan de criterios de interpretación claros y acotados para evitar aplicaciones abusivas o equívocas de las normas en cuestión. De lo contrario, las disposiciones normativas podrían generar afectaciones indebidas a la libertad de expresión incluso cuando persiguen objetivos legítimos y buscan abordar problemáticas serias y sistémicas—como es el caso.

En particular, encontramos problemas del orden de la *legalidad* en los artículos 2, 7, y 8.

La definición genérica del artículo 2 sobre violencia digital contra las mujeres por razones de género es problemática en algunos aspectos. En particular, el daño *simbólico* es una categoría amplia que no tiene una definición específica ni unificada. No existen estándares ni criterios claros respecto a cómo se demuestra este tipo de daño, y es especialmente problemática esa falta de precisión si la definición fuese a utilizarse como fundamento de acciones restrictivas a

[1] CIDH, «Marco jurídico interamericano del Derecho a la Libertad de Expresión», Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2009, párr. 67.

la libertad de expresión. Una forma de entender el concepto es que la violencia simbólica se materializa en expresiones que perpetúan los estereotipos de género.[2] Sin embargo, la amplitud de esta lectura permite el ingreso a la prohibición de conductas éticamente reprochables y socialmente problemáticas, pero permitidas desde el punto de vista legal o cuya ilegalización sería costosa en términos de libertades individuales[3].

Una posible vía de escape de este dilema la ofrece el artículo 7 sobre manifestaciones de la violencia digital, un conjunto de definiciones que podrían leerse como delimitando distintos tipos de violencias que pueden sufrir las mujeres en el ámbito digital. Éstas definiciones son más precisas y acotadas, y más pasibles de satisfacer los exigentes requisitos del test tripartito. Además, al definir a las violencias que pueden sufrir las mujeres de manera múltiple, se hace más fácil la tarea de distinguir entre distintas medidas para combatirlas, que pueden ir desde el castigo y el derecho penal en los casos más claros y graves—como, por caso, la difusión sin consentimiento de imágenes íntimas—hasta medidas tendientes a la educación en la tolerancia y la no discriminación, el combate de estereotipos de género y otras medidas que pueden combatir la prevalencia social de ciertos tipos de discursos que el estado puede estar legitimado a combatir discursivamente sin cercenar el derecho a la libertad de expresión de quienes los sostengan. De todas formas, encontramos que estas definiciones pueden ajustarse para alcanzar una mayor claridad y precisión en los siguientes literales:

Las manifestaciones enunciadas en el artículo 7 son valiosas y útiles para acotar la definición de violencia digital contra las mujeres, que en determinadas circunstancias puede constar de una ambigüedad riesgosa para la libertad de expresión. Creemos que es conveniente que las manifestaciones de violencia allí descritas sirvan como criterio evaluador de la conducta o expresión jurídicamente reprochada. Por tanto, solicitamos ajustar para mayor claridad, los siguientes literales:

- Literal g: describe como manifestación "usar software espías en dispositivos electrónicos que permiten el control remoto de cámaras, micrófonos o geolocalización". No obstante, existen spywares con mayores capacidades de intromisión, de manera que la descripción tal y como está puede dejar por fuera

[2] Es posible inferir que este tipo de daño es el producto de la violencia simbólica, conceptualizada por Bourdieu como "violencia que arranca sumisiones que ni siquiera se perciben como tales apoyándose en unas «expectativas colectivas», en unas creencias socialmente inculcadas". *Ver* Bourdieu, Pierre (1999), Intelectuales, política y poder, Buenos Aires, Eudeba.

[3] Cfr. Afrofeminas, «Afroféminas5 ejemplos de violencia simbólica», Afrofeminas, *Afroféminas*, Disponible en https://afrofeminas.com/2022/04/10/5-ejemplos-de-violencia-simbolica/.

atentados graves a la intimidad de las mujeres. Por ejemplo, el famoso software Pegasus, desarrollado por la empresa Israelí NSO Group, es "capaz de descifrar confiablemente las comunicaciones encriptadas de los iPhones y los teléfonos inteligentes Android".[4] De forma similar, con el uso del spyware Graphite, desarrollado por la empresa Paragon Solutions, "el operador del programa espía tiene acceso total al teléfono, incluso puede leer los mensajes que se envían a través de aplicaciones cifradas como WhatsApp y Signal".[5]

Cabe señalar que los spyware no son el único tipo de tecnología que representa riesgos de graves intromisiones sobre la privacidad de las personas y que son susceptibles de ser usadas de manera ilegal en razón del género de la víctima. Algunas técnicas de inteligencia que se apoyan en distintas tecnologías digitales, como el SIGINT o inteligencia de señales, han sido usadas de manera abusiva e ilegal para espiar a personas, sin fundamentos legales, por parte de funcionarios públicos. Este fue el caso del llamado *loveint* realizado por empleados de la NASA en 2013.[6] Si bien la conclusión del caso no fue pública, este tipo de situaciones deben ser investigadas y sancionadas aplicando una perspectiva de género interseccional, que examine las relaciones de poder que intervienen en las prácticas abusivas e ilegales al usar tecnologías de vigilancia.

- Literal *h* incluye el verbo rector de *manipular*; sin embargo, hay circunstancias bajo las cuáles se puede realizar manipulación de datos con fines lícitos. Entendiendo que la acción en cuestión se refiere al "proceso de limpiar, normalizar y preparar los datos para que puedan ser analizados y visualizados correctamente"[7] para los fines de la

[4] The New York Times (2022) Pegasus: esto aprendimos tras un año de investigar al programa espía más potente del mundo. Disponible en: https://www.nytimes.com/es/2022/01/28/espanol/pegasus-israel-nso-espionaje.html

[5] R3D (2025) Empresa israelí de spyware se utiliza para espiar a periodistas que denuncian el fascismo. Disponible en: https://r3d.mx/2025/02/05/empresa-israeli-de-spyware-se-utiliza-para-espiar-a-periodistas-que-denuncian-el-fascismo/

[6] The Washington Post (2013) LOVEINT: When NSA officers use their spying power on love interests. Disponible en: https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/

[7] Curso ofrecido por el programa de formación docente y educación continua de la CUAIEED-UNAM en el mes de agosto de 2022. Introducción a la manipulación de datos. Disponible en: https://mooc-unam-publico.github.io/curso-datos/S3-procesamiento/S3P1-introduccion.html

presente ley, tiene más relevancia el uso del dato que la simple manipulación del mismo. Por ejemplo, si se quisiera hacer un estudio sobre la composición del género del poder judicial se requeriría manipular datos personales. La definición entonces abarca más de lo necesario.

- Literal *m*, es importante señalar que una de las principales preocupaciones sobre los sistemas basados en inteligencia artificial, desde una perspectiva de derechos humanos, es su capacidad de reproducir y perpetuar sesgos discriminatorios que no se limitan únicamente a aquellos en razón del género. De esta manera, es imperativo que los sistemas de inteligencia artificial sean analizados y tratados con enfoques diferenciales amplios que permitan la protección del derecho a la igualdad de todas las personas; y que, cuando se trate de sistemas que faciliten conductas de violencia basada en género, estas situaciones se enfrenten con una perspectiva de género interseccional.

Otro aspecto de la ley que podría beneficiarse de una mayor precisión en el lenguaje se relaciona al artículo 8. El estudio realizado por Maricarmen Sequera de TEDIC, que el CELE publicó el año pasado, demuestra los riesgos de normas redactadas de manera excesivamente vagas. Allí, nuestra colega estudió cómo la aplicación tergiversada de la Ley 5777/16 en Paraguay resultó en un mecanismo indirecto de censura desplegado por personas poderosas para acallar voces críticas.

> "Las regulaciones ambiguas pueden resultar en decisiones arbitrarias que comprometan injustamente el derecho a la libertad de expresión, especialmente para las y los usuarios individuales que participan en el debate público únicamente con la fuerza de sus argumentos. Las leyes ambiguas pueden tener un impacto significativo en este creciente grupo de personas, cuya inclusión en el debate público es una de las principales ventajas de Internet como espacio de comunicación global.[8]"

Con base en lo anterior, consideramos que debe limitarse el alcance de los literales *a*, *b* y *c* del artículo 8, ya que su amplio contenido puede restringir prácticas y discursos que—aunque puedan considerarse cuestionables—son legítimos bajo el marco interamericano de libertad de expresión. En el literal *d* del mismo artículo, consideramos que las capacitaciones deben versar además de la prevención, de prácticas conscientes de no revictimización y que estas

[8] Maricarmen Serquera, "Violencia de género en línea y libertad de expresión. Estudio de seis casos en Paraguay", Artículo de investigación No. 59, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024). Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5157887.

deben ser proporcionadas a todos los funcionarios públicos que puedan intervenir con competencia en la generación de políticas para prevenir, mitigar y atender la violencia digital de género, y aquellos que se encarguen particularmente de manejar los casos.

Hay otros conceptos destacados que se desarrollan en el texto legal que requieren una definición detallada para delimitar su alcance. Específicamente, solicitamos que se describa qué es lo que se entiende como "uso de tecnologías", especialmente porque en la actualidad no existe claridad sobre el concepto del fenómeno que pretende ser regulado y, por el contrario, este tipo de violencia ha sido llamada *violencia digital, violencia facilitada por la tecnología* y *violencia en línea,* en distintos contextos, lo que ha generado confusión. En este ámbito, como resultado de un trabajo de investigación que tuvo como objetivo identificar el panorama de definiciones, conceptos y manifestaciones sobre la violencia digital, organizaciones de la sociedad civil mapearon el siguiente concepto sobre uso de tecnología:

> "Uso de la tecnología como medio de perpetración: Implica el uso de las tecnologías de la información y la comunicación (TIC) para llevar a cabo acciones que buscan controlar, intimidar o dañar a las sobrevivientes y podría constituir un continuo de la violencia fuera de línea y la discriminación estructural existentes.[9]"

Encontramos que esta definición es más acotada y podría ser útil a los fines de la ley modelo.

Marco general de la responsabilidad de los intermediarios

Un punto que merece especial atención de la ley modelo es el capítulo III, que dispone normas generales sobre regulación de plataformas incluyendo la obligación de mantener representaciones legales en los países en los que opera, puntos de contacto, obligaciones específicas, entre otros requerimientos. Este tipo de requisitos no son aún objeto de un consenso extendido en la región ni surgen de manera clara de ningún *modelo* que pueda seguirse con claridad[10]. Es importante que las leyes modelo promuevan la racionalización de la actividad legislativa y el debate democrático que se materializa a través de los trámites internos que estipulan las constituciones de los Estados de la región para la aprobación de los textos

[9] TEDIC (2024) From theory to practice building and testing framework for definitions of online gender-based violence and other terms. Disponible en:
https://www.tedic.org/wp-content/uploads/2024/07/Framework-definitions-OGBV-2.pdf

[10] Matías González y Belén Portugal, "La exigencia de presencia local a las empresas TIC: una mirada desde el derecho internacional de los derechos humanos y el derecho económico internacional", Artículo de investigación No. 55, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2022).

legislativos. Es deseable, entonces, que el texto propuesto satisfaga una estricta congruencia temática que garantice que la materia sometida a debate se extienda a lo largo de las disposiciones que constituyen la propuesta. Este principio—aceptado, por ejemplo, en la jurisprudencia constitucional de Colombia[11]—permite que no se introduzcan en textos legislativos cuestiones ajenas a la materia central que requerirían, por su distanciamiento, un debate propio y específico. La ley modelo, al avanzar sobre cuestiones generales de regulación de plataformas, avanza en una dirección que excede al MESECVI y a la problemática de la violencia contra las mujeres, e ingresa en una discusión más amplia sobre la cual aún no hay acuerdos extendidos.

La regulación precisa de las plataformas en Internet debe ser sometida a un riguroso debate que permita desarrollar criterios comunes para identificar prácticas y obligaciones que se puedan imponer de manera efectiva sobre las empresas transnacionales que operan los servicios de Internet que tienen cuotas variables de responsabilidad sobre fenómenos como la violencia de género en línea, la desinformación, el discurso de odio, etcétera. Este diálogo aún no ha ocurrido, y debería incluir a las múltiples partes interesadas en el ecosistema de información que podría verse afectado por este tipo de normas. En este sentido, hay importantes iniciativas en curso como el *Global Digital Compact* o las iniciativas de UNESCO sobre regulación de plataformas que fueron objeto de críticas—precisamente—por la falta de diálogo o deliberación en su proceso de gestación. El proceso de consultas de la ley modelo que aquí comentamos puede satisfacer ese requisito, pero no es, ni ha sido, lo suficientemente amplio y abarcativo por la sencilla razón de que la problemática que ha procurado abordar es específica y concreta. Y las personas que han participado de este proceso no son las especialistas relevantes en materia de regulación de plataformas y gobernanza de Internet.

El escenario regulatorio a nivel global está, actualmente, atravesando un profundo proceso de cambio. La indemnidad que se ha dado a las empresas de Internet en Estados Unidos a través de la sección 230 de la *Communication Decency Act* de 1996 ha sido modificada por medio de normas limitantes de la responsabilidad civil que son menos absolutas—como la Directiva de Comercio Electrónico de la Unión Europea del 2000—o por medio de la adopción de criterios de interpretación jurisprudencial[12]. La Digital Services Act de la Unión Europea del

[11] Corte Constitucional. Sentencia C-714/2001. M.P. Rodrigo Escobar. Disponible en: https://www.corteconstitucional.gov.co/relatoria/2001/C-714-01.htm

[12] Álvarez Ugarte, R.; Vitaliani, E., «Redes de influencia: análisis de la jurisprudencia civil argentina en materia de responsabilidad de intermediarios», Revista Chilena de Derecho y Tecnología, vol. 11, n.º 2, 2022, págs. 147-182.

2022 podría convertirse en un modelo regulatorio a seguir pero ese camino está plagado de incertidumbres y riesgos, vinculados—especialmente—a las diferentes infraestructuras institucionales que podrían encargarse de administrar un régimen legal tan complejo y las diferencias sustantivas entre legislaciones marco regionales y las legislaciones locales[13]. Aún es demasiado pronto para conocer con precisión la dirección de los cambios. Al optar por caminos específicos, la ley modelo avanza en una dirección problemática que no goza—aún—de consenso suficiente.

Señalada la precaución anterior, sí consideramos pertinente identificar algunos temas puntuales de la sección.

- Artículo 18: la disposición crea de manera indirecta una obligación de monitoreo activo, conexo al deber de notificación; no obstante, no existe un marco sobre la manera en que que actores privados deben realizar tal acción ni determina de manera clara qué tipo de violencia es aquella sobre la que recae la obligación de notificación.
- Artículos 19 y 21: cuando dice órdenes estatales debería decir órdenes de las autoridades *judiciales*[14]. Ello así por los requerimientos de imparcialidad e independencia que deben tener medidas que afecten a la libertad de expresión. Además, las disposiciones del artículo 19 pueden conllevar a un efecto silenciador preocupante, derivados de la obligación de "frenar, ocultar o eliminar materiales", especialmente, porque los criterios de la norma dan un margen de discrecionalidad uy amplio.
- Artículo 22: utiliza términos como "transparencia*"y "ética algorítmica" que no tienen una definición legal clara y—por consecuencia—podrían ser abusados. El artículo también habla de otorgar o retirar el consentimiento de manera consciente, sin detenerse a explicar qué significa eso de manera precisa. Por otro lado, en el segundo párrafo la palabra "dañino" podría cambiar por otra más precisa como "ilegal" o "que causa un daño a los derechos de niñas, adolescentes y mujeres". El texto lograría, así, más precisión.
- El artículo 24: pide a las plataformas que den razones cuando los contenidos son objeto de moderación. Si bien estamos de acuerdo en que eso es deseable, la realidad

[13] González Mama, M.; Alvarez Ugarte, R., «Modelización regulatoria. Palpitando la influencia de la Digital Services Act en América Latina», Artículo de Investigación No. 63, Centro de Estudios en Libertad de Expresión, Buenos Aires, Argentina, 2025.

[14] CIDH, «Libertad de expresión e Internet», Comisión Interamericana de Derechos Humanos, Washington, DC, 2013, párr. 165; CIDH, «Estándares para una Internet libre, abierta e incluyente», Relatoría Especial para la Libertad de Expresión de la CIDH, Washington D.C., 2017, párr. 89.

de la moderación de contenidos a escala es que los contenidos de los usuarios son objeto de sistemas de automatizados de moderación que admiten—en el mejor de los casos—una revisión posterior, o una identificación muy precaria de los motivos por los cuales cierta pieza fue sometido a algún tipo de moderación. Si bien estamos de acuerdo en que ésto sería deseable, el volumen de la información que es objeto de moderación no permitiría satisfacer—al menos plenamente—los requisitos del artículo.

- Artículo 40: pide la creación de una Autoridad Nacional Administrativa que ejerza funciones de policía y control sobre las plataformas de Internet, de un modo que podría ser problemático dependiendo el contexto. América Latina no tiene buenas tradiciones de organismos independientes en la esfera administrativa, y el potencial de abusos de este tipo de órganos es alto. Es un punto a considerar, especialmente en el marco de nuestra objeción más genérica de avanzar en una línea general de "gobernanza de plataformas" que no goza de consenso entre los expertos, más o menos inspirada en una ley marco europea—la *Digital Services Act*—cuyo proceso de implementación es aún incipiente y dudoso.