Violencia de género en entornos digitales. Tensiones a propósito de su criminalización

Digital gender violence. Tensions regarding its criminalization

María Fernanda García[1]
ORCID: 0000-0002-3197-2625
DOI: https://doi.org/10.5281/zenodo.18209254

Fecha de recibido: 28 de noviembre de 2025 / Fecha de aprobación: 20 de diciembre de 2025

Resumen

La violencia de género en entornos digitales constituye un fenómeno global en expansión, derivado tanto de las estructuras históricas de desigualdad que afectan a mujeres, infancias y diversidades sexo-genéricas, como de la hiperconectividad generada por el uso masivo de las tecnologías de la información y la comunicación (TIC). La digitalización acelerada durante la pandemia de COVID-19 evidenció que, a medida que más mujeres acceden a los espacios virtuales, crecen también los casos de ciber-violencias. En este contexto, las redes sociales se consolidan como escenarios donde se configuran vínculos y prácticas sexuales, ahora mediados tecnológicamente. Se reeditan comportamientos ya conocidos bajo nuevas formas que se amplifican por la virtualidad. Este escenario plantea importantes desafíos para el derecho penal contemporáneo, que debe repensar qué conductas perseguir y cómo garantizar respuestas estatales eficaces frente a las violencias digitales.

Palabras Clave

Derecho al olvido; entorno digital; Ley Olimpia; libertad de expresión; violencia de género.

Abstract

Gender violence in digital environments is an expanding global phenomenon, stemming from both historical structures of inequality affecting women, children and gender-diverse people, and from the hyperconnectivity generated by the massive use of information and communication technologies (ICTs). The accelerated digitization during the COVID-19 pandemic demonstrated that, as more women access virtual spaces, the incidence of cyber-violence also increases. In this context, social networks are becoming established as platforms where technologically mediated sexual relationships and practices are configured, perpetuating pre-existing behaviors in new forms amplified by virtuality. This scenario poses significant challenges for contemporary criminal law, which must rethink what conduct to prosecute and how to guarantee effective state responses to digital violence.

words

Digital gender violence; freedom of expression; Olimpia Law; right to be forgotten.

[1] Abogada (UNLP-Argentina), Especialista en Derecho Penal (Universidad de Salamanca-España), Magister en Derechos Humanos (UNLP-Argentina), Doctoranda en Derecho (UP-Argentina). Correo: mfernandagarciacampos@gmail.com

Tabla de contenido

Introducción

El presente artículo aborda la violencia digital por motivos de género desde un enfoque de derechos humanos y perspectiva de género. El objetivo es examinar las transformaciones que las tecnologías de la información y la comunicación (TIC) introducen en las relaciones de poder sexo-genéricas, las prácticas de violencia y las respuestas institucionales.

La violencia por motivos de género en entornos digitales constituye en la actualidad un fenómeno global en expansión, producto de la convergencia entre la persistente violencia estructural que atraviesa a mujeres, infancias y personas pertenecientes al colectivo LGTBIQ+, y la hiperconectividad derivada del uso masivo de las tecnologías de la información y la comunicación (TIC).

El proceso de digitalización acelerada, profundizado a partir de la pandemia de COVID-19, puso de manifiesto una correlación preocupante: a medida que más mujeres y niñas acceden a espacios digitales, aumenta en proporción la incidencia de la violencia digital por motivos de género (ONU Mujeres, 2021). Esa forma de violencia, aunque se manifiesta en un entorno distinto, reproduce las mismas estructuras de desigualdad, dominación y control que operan en el espacio físico, trasladando las lógicas patriarcales al ámbito virtual y generando nuevas modalidades de vulneración de derechos fundamentales, entre ellos la intimidad, la dignidad, la integridad personal y la libertad sexual.

En ese contexto, las redes sociales y las plataformas digitales se configuran como escenarios centrales de socialización, donde se redefinen los modos de vinculación afectiva y sexual. La sexualidad se expresa hoy a través de imágenes, sonidos y narrativas digitales que amplifican la representación del deseo y la exposición del cuerpo, en ocasiones disociadas de la corporalidad. Sin embargo, la mediación tecnológica también habilita nuevas formas de violencias simbólicas y sexuales, como la difusión no consentida de material íntimo o el acoso digital, prácticas que tienen un impacto emocional y social que merece atención (Citron, 2022).

La codificación penal clásica enfrenta, en consecuencia, el desafío de adaptar sus categorías y principios a esos nuevos marcos de actuación. El derecho penal se ve interpelado por los nuevos modos de interacción interpersonal mediada por TICs, que complejizan la delimitación del bien jurídico protegido, la jurisdicción aplicable y la atribución de responsabilidad. De allí surgen interrogantes cruciales: ¿qué comportamientos deben ser objeto de persecución penal?, ¿cuáles son los límites legítimos de la intervención estatal en la regulación del ciberespacio?, ¿cómo garantizar la protección de las víctimas sin afectar la libertad de expresión y el derecho a la información?

En respuesta a esos desafíos, diversos países han avanzado en la tipificación penal de las violencias digitales de género, destacándose el caso de México con la Ley Olimpia (Decreto publicado en el Diario Oficial de la Federación el 1 de junio de 2021[2]), que incorporó el delito de violación a la intimidad sexual en el Código Penal Federal y en los códigos locales. Esa normativa marcó un hito regional al reconocer expresamente la violencia digital como una forma de violencia de género, inspirando reformas similares en otros países latinoamericanos, entre ellos Argentina, donde se debate el Proyecto de Ley Belén (Expediente 2757-D-2022), orientado a criminalizar la difusión no consentida de material íntimo y otras conductas de acoso digital.

Desde el plano teórico, autoras como Danielle Citron (2022) y Mary Anne Franks (2019) han advertido la necesidad de reformular los marcos tradicionales del derecho penal frente a esa clase de violencias. A modo de referencia, Citron, en su obra *The Fight for Privacy*, sostiene que la violencia digital que sufren las mujeres debe entenderse como una extensión de la desigualdad estructural que atraviesan en el ámbito público y privado, lo que requiere un enfoque diferencial y particular por parte de la ley.

En este marco, el presente trabajo propone una aproximación analítica y crítica al fenómeno de la violencia digital de género, bajo la cual repasar su conceptualización jurídica, su tratamiento normativo en el derecho comparado y los desafíos que plantea para los sistemas penales contemporáneos. Asimismo, se delinean posibles vías de acción estatal orientadas a fortalecer las políticas públicas de prevención, investigación y reparación, garantizando una respuesta integral, coordinada y respetuosa de los estándares internacionales de derechos humanos.

1. Violencia de género digital. Concepto y conductas

La violencia de género digital comprende una amplia gama de conductas que reproducen y amplifican las desigualdades estructurales de género en entornos virtuales. Según la Relatoría Especial de la ONU sobre la violencia contra la mujer (A/HRC/38/47, 2018), se trata de "todo acto de violencia por razón de género contra las mujeres cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este" (párr. 23).

Este fenómeno se enmarca dentro del concepto más amplio de violencia contra las mujeres reconocido en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará, 1994) y en la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, 1979), y presenta características específicas: su reproducción inmediata, la volatilidad de los contenidos, la facilidad de alteración/modificación, el anonimato de los agresores y la transnacionalidad de las conductas. Todo ello dificulta su investigación y sanción, demandando estrategias estatales coordinadas e internacionales.

Pueden mencionarse algunas conductas que forman parte de dicho universo, respecto de las cuales se ha reconocido su existencia en documentos internacionales

[2] Más allá de la referencia a ese decreto de 2021, cabe aclarar que la denominada "Ley Olimpia" es el nombre de un proceso legislativo más amplio y extendido en el tiempo que reconoció como objetivo el reformar los códigos penales estatales, el Código Penal Federal y las leyes de acceso de las mujeres a una vida libre de violencia a lo largo y ancho de todo México. Es por ello que en el presente trabajo se efectúan menciones a reformas legislativas ocurridas al amparo de dicha ley que no se corresponden con la fecha señalada y que, incluso, obedecen a momentos anteriores a dicho año.

de derechos humanos de las mujeres e, incluso, algunos Estados han dictado normativas específicas.

a) *Difusión no consentida de material íntimo:* Consiste en la publicación o amenaza de publicación de imágenes, audios o videos de contenido sexual sin consentimiento. El material suele haber sido compartido en un contexto privado (por ejemplo, mediante *sexting*[3]) y luego es utilizado para humillar, coaccionar o controlar a la víctima (MESECVI-ONU Mujeres, 2022, p. 31). La Ley Olimpia en México, a través de la incorporación del artículo. 199 *octies* al Código Penal Federal, tipifica esa conducta como "violación a la intimidad sexual".
b) *Doxeo:*[4] El *doxeo* implica revelar o publicar información personal o privada de una persona sin su consentimiento, como direcciones, números de teléfonos personales o de familiares. El Informe de la Relatora Especial (2018) contempla aquellas "situaciones en que la información y los datos personales obtenidos por el autor del abuso se hacen públicos con intención dolosa, en una clara violación del derecho a la intimidad" (párr. 36).
c) *Pornovenganza:* La denominada pornovenganza es la difusión no consentida de material sexual con el objetivo de difamar, castigar o humillar a la víctima. Aunque el término sugiere una motivación de represalia, la doctrina feminista lo critica por su sesgo culpabilizador ya que contendría una justificación implícita del actuar del agresor. Más allá de esto, cierto es que el término pornovenganza es el que ha logrado extenderse en el discurso social e incluso ha sido receptado en documentos internacionales de derechos humanos de las mujeres como es el referido informe de la Relatoría Especial de 2018. Dicho informe reconoce esa práctica como una manifestación de violencia digital de género y recomienda su penalización específica (párr. 41).
d) *Upskirting* y *downblousing:* Estas prácticas consisten en captar imágenes íntimas del cuerpo de una persona sin su consentimiento —por debajo de la falda o desde el escote— en espacios públicos. Algunos países como Reino Unido (2019) las tipifican expresamente como delitos contra la intimidad. Su existencia refleja la persistencia de la cosificación del cuerpo femenino y la mirada masculina como instrumento de dominación.
e) *Ciberacoso sexual:* El ciberacoso sexual comprende toda conducta verbal o no verbal de naturaleza sexual no deseada que genere un entorno hostil, intimidatorio o humillante. Incluye mensajes, comentarios o imágenes de contenido sexual enviados por redes sociales o correo electrónico. Según el Informe de la Relatoría Especial (2018) el objetivo particular que persigue esta clase de conductas es "crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo" (párr. 40). El acoso puede realizarse bajo formas muy diversas. Por ejemplo, a través del envío de emails o correos electrónicos, mensajes en redes sociales (públicos o privados) o, incluso, mediante el envío de múltiples "solicitudes de amistad". A diferencia del

[3] Práctica que contempla el envío consentido de mensajes, fotos o vídeos de contenido íntimo a través de medios digitales.
[4] El término *doxeo* o *doxing* proviene de un neologismo en referencia a la abreviatura del vocablo documentos en idioma inglés (docs).

ciberhostigamiento, el ciberacoso puede configurarse con un solo acto (ONU Mujeres, 2021. MESECVI-ONU Mujeres, 2022, p. 30).

f) *Ciberbullying:* El *ciberbullying*, considerado un subtipo de ciberacoso, es una forma de violencia digital que busca en concreto difamar, insultar o ridiculizar a una persona mediante redes sociales o mensajería. Cuando está dirigido a mujeres suele contener un componente sexualizado o misógino. Cuando el acoso reconoce como escenario el ámbito laboral, es correcto utilizar el término *cibermobbing* (MESECVI-ONU Mujeres, 2022, p. 13).

g) *Ciberhostigamiento:* El ciberhostigamiento, o ciberintimidación o acecho digital se configura cuando una persona realiza actos reiterados de intimidación o vigilancia en línea. La particularidad es que el conjunto de actos conforma un patrón de conducta digital abusiva que termina por generar la sensación de inseguridad virtual de las víctimas. Todo ello, más allá de que uno solo de dichos actos, considerado en su individualidad, no tenga dicha capacidad intimidatoria (Relatoría Especial, 2018, párr. 39. MESECVI-ONU Mujeres, 2022, p. 29).

h) *Amenazas virtuales:* Comprenden expresiones de violencia o intimidación proferidas a través de medios digitales. Pueden ser coactivas —si buscan forzar a la víctima a realizar o tolerar algo— o simples —si buscan generar miedo o sufrimiento. El anonimato y la viralización dificultan su investigación (Relatoría Especial, 2018, párrs. 30 y 31. MESECVI-ONU Mujeres, 2022, p. 35).

i) *Discurso de odio de género y trolling:* La difusión de mensajes misóginos o transfóbicos en línea constituye una forma de violencia simbólica que busca excluir a las mujeres del debate público digital. Los ataques coordinados o '*trolleos*' colectivos generan autocensura y miedo, restringiendo la libertad de expresión y participación política a través de campañas coordinadas de acoso y desprestigio (Relatoría Especial, 2018, párr. 37). ONU Mujeres (2021) advierte que esa forma de violencia digital tiene efectos de silenciamiento y autocensura sobre las víctimas, afectando su libertad de expresión y participación en debates públicos.

j) *Acceso no consentido a sistemas informáticos:* El acceso ilegítimo a cuentas o dispositivos electrónicos de una persona sin su consentimiento, con el propósito de controlar, vigilar o difundir información privada, constituye una violación a la intimidad y a la seguridad digital (MESECVI-ONU Mujeres, 2022, p. 33). El Convenio de Budapest sobre Ciberdelincuencia (2001) tipifica esa conducta como delito informático.

k) *Abusos sexuales por medios telemáticos y explotación sexual y/o trata de mujeres facilitada por las TICs:* Tanto los abusos sexuales como la explotación sexual y la trata de personas son delitos que comprometen físicamente a las personas involucradas. Sin embargo, puede ocurrir que se perfeccionen estos crímenes por medio del uso de TICs. En el caso de los abusos, es posible que se empleen plataformas digitales para coaccionar o engañar a una víctima a realizar actos sexuales, sin contacto físico directo. En el segundo de los supuestos mencionados, los casos de explotación sexual, el uso de las TICs puede estar

direccionado, por ejemplo, a la captación de víctimas a través de ofertas laborales engañosas (MESECVI-ONU Mujeres, 2022, p. 36).

l) *Suplantación y robo de identidad digital:* Consiste en la creación de perfiles falsos o la apropiación de identidades digitales para difundir contenido sexual o dañar la reputación de la víctima. Esta práctica atenta contra el derecho a la identidad digital y puede combinarse con otras formas de violencia, como la sextorsión o la difamación (MESECVI-ONU Mujeres, 2022, p. 34).

m) *Sextorsión:*La sextorsión combina elementos de coerción sexual y abuso de poder. Puede adoptar dos formas: una extorsiva —cuando el agresor exige dinero o favores a cambio de no difundir contenido sexual— y otra estructural —cuando se ejerce poder para obtener beneficios sexuales. En ambos casos, se trata de una manifestación de la violencia sexual y de la corrupción de género en contextos digitales. La conceptualización de ese fenómeno se encuentra discutida dentro de los feminismos jurídicos. Algunas voces lo consideran como una extorsión o chantaje a través del cual se amenaza a la víctima con la publicación de material audiovisual de contenido sexual, con el fin de obtener algo a cambio, diferenciándose de la pornovenganza en su elemento coercitivo (Relatoría Especial, 2018, párr. 35. MESECVI-ONU Mujeres, 2022, p. 33. Sequeira, 2021).

Otras perspectivas hablan de un abuso de poder -ejercido generalmente por varones- para obtener una ventaja o beneficio sexual, abordándola como una forma de corrupción y de violencia de género, una expresión de la llamada corrupción sexual, en la cual el sexo, en lugar del dinero, es la moneda de cambio del soborno (Asociación Internacional de Mujeres Juezas, 2012. Mazzaferri, Roteta, 2022).

2. Derechos afectados por la violencia digital

A raíz de lo desarrollado hasta aquí queda en evidencia que la violencia de género digital vulnera una multiplicidad de derechos humanos reconocidos en los principales instrumentos internacionales de protección, que imponen obligaciones jurídicas vinculantes a los Estados parte. Entre ellos, la Convención CEDAW (1979) y la Convención de Belém do Pará (1994) establecen el deber estatal de eliminar toda forma de discriminación y de prevenir, investigar y sancionar los actos de violencia que afecten a las mujeres en cualquier ámbito, entre los que queda incluido el digital. A su vez, la Convención Americana sobre Derechos Humanos (1969), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP, 1966) y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC, 1966), al contemplar la protección de derechos fundamentales como la integridad, la libertad, la privacidad y la igualdad, amplían el paraguas convencional.

2.1. Derecho a la dignidad y a la igualdad

La dignidad humana constituye la base de todos los derechos humanos y ha sido reconocida expresamente por la Declaración Universal de Derechos Humanos (1948, art. 1) y la Convención Americana sobre Derechos Humanos (art. 11). La violencia digital, al exponer, humillar o degradar públicamente a las mujeres, vulnera este principio fundamental. Además, reproduce y refuerza las desigualdades

estructurales de género, contrariando la obligación de los Estados de garantizar la igualdad sustantiva prevista en los artículos 2 y 5 de la Convención CEDAW.

2.2. Derecho a la integridad personal

El artículo 5 de la Convención Americana protege el derecho a la integridad física, psíquica y moral. Las agresiones en línea, como la difusión de material íntimo, el ciberacoso o la sextorsión, generan daños psicológicos significativos que afectan el bienestar emocional y la seguridad personal. El Comité CEDAW ha reconocido que la violencia de género, en todas sus formas, constituye una violación de este derecho, y que los Estados tienen la obligación de adoptar medidas efectivas para su prevención, su persecución y sanción y para la reparación integral a las víctimas (Recomendación General 35, 2017, ptos. 29, 31 y 33).

2.3. Derecho a la intimidad y a la privacidad

El derecho a la privacidad y a la protección de datos personales está garantizado en el artículo 11 de la Convención Americana que reconoce que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". En iguales términos lo hace el Pacto Internacional de Derecho Civiles y Políticos (artículo 17).

La violencia digital —en particular la difusión no consentida de material íntimo o el acceso ilegítimo a dispositivos y cuentas personales— constituye una clara injerencia arbitraria en la vida privada de las personas. La Relatoría Especial para la Libertad de Expresión de la CIDH (2017, ptos. 192 y 194) ha sostenido que las acciones estatales frente a esas violaciones deben ser inmediatas, proporcionadas y respetuosas de los derechos digitales.

2.4. Derecho a la libertad y seguridad personales

El artículo 7 de la Convención Americana reconoce el derecho de toda persona a la libertad y a la seguridad personales. Las amenazas, hostigamientos y persecuciones virtuales que generan miedo o coacción en las personas víctimas afectan de forma directa este derecho. El deber de los Estados no se limita a sancionar las agresiones consumadas, sino que incluye la prevención y la protección efectiva de las potenciales víctimas, conforme al principio de debida diligencia en materia de violencias basadas en el género establecido por la Corte Interamericana en el caso "González y otras (´Campo Algodonero´) vs. México" (2009).

2.5. Derechos sexuales y reproductivos

El derecho al goce del más alto nivel posible de salud física y mental (art. 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales) incluye los derechos sexuales y reproductivos, reconocidos como derechos humanos por el Comité DESC (Observación General 22, 2016, pto. 1). La violencia digital que involucra la exposición, coerción o manipulación sexual constituye una violación directa de esos derechos. La falta de protección adecuada, por ejemplo, frente a la difusión de contenido íntimo o la sextorsión, afecta la autonomía sexual y la capacidad de las mujeres para decidir con libertad sobre su cuerpo y su sexualidad.

2.6 Obligación estatal de debida diligencia

La Convención de Belém do Pará (art. 7) y la Recomendación General 35 del Comité CEDAW establecen la obligación de los Estados de actuar con debida diligencia para prevenir, investigar, sancionar y reparar los actos de violencia contra las mujeres, dentro de la cual debe entenderse incluida la violencia digital. La falta de medidas adecuadas de prevención o la ineficacia en la investigación comprometen la responsabilidad internacional del Estado. La Corte Interamericana, en casos como el ya mencionado "González y otras vs. México", afirmó que el deber de debida diligencia es una obligación positiva de garantía que no se satisface únicamente con la sanción formal de normas por parte de los Estados, sino con su aplicación efectiva y con políticas públicas que aseguren la protección real de las víctimas.

3. Legislación aplicable y estándares internacionales en materia de violencia de género digital

3.1. Contexto internacional y obligaciones estatales

De lo expuesto hasta aquí se interpreta que el abordaje jurídico-normativo de la violencia de género digital encuentra su fundamento en los compromisos asumidos por los Estados dentro del Sistema Universal y el Sistema Interamericano de Derechos Humanos. Instrumentos como la Convención CEDAW, la Convención de Belém do Pará y la Convención Americana sobre Derechos Humanos obligan a los Estados a actuar con la debida diligencia reforzada para prevenir, investigar, sancionar y reparar toda forma de violencia contra las mujeres, incluso aquellas mediadas por las TICs.

La mencionada Recomendación General 35 del Comité CEDAW introdujo una ampliación sustantiva al concepto de violencia de género, al incorporar expresamente las formas de violencia digital y tecnológica: "La violencia por razón de género contra la mujer se produce en todos los espacios y esferas de la interacción humana, ya sean públicos o privados, entre ellos los contextos de la familia, la comunidad, los espacios públicos, el lugar de trabajo, el esparcimiento, la política, el deporte, los servicios de salud y los entornos educativos, y en la redefinición de lo público y lo privado a través de entornos tecnológicos, como las formas contemporáneas de violencia que se producen en línea y en otros entornos digitales" (pto. 20).

Por su parte, la Corte Interamericana de Derechos Humanos ha consolidado estándares claros sobre la obligación estatal de proteger a las mujeres frente a la violencia por motivos de género, como en los casos "Campo Algodonero vs. México" (2009) y "Fernández Ortega vs. México" (2010), estándares que resultan de aplicación en la materia más allá de que los referidos precedentes no versen sobre supuestos de violencias digitales. Allí se estableció que los Estados deben adoptar políticas públicas, legislación adecuada y mecanismos judiciales efectivos para garantizar el derecho de las mujeres a vivir una vida libre de violencia.

Esos estándares de derechos humanos de las mujeres que brindan la normativa y jurisprudencia internacionales se aplican a la violencia de género digital, ya que son una derivación de los principios analizados en el apartado anterior de igualdad sustantiva y no discriminación, privacidad y protección de datos personales, libertad personal y no revictimización.

3.2. El caso puntual de México: Ley Olimpia y Ley Ingrid

México fue el primer país de América Latina en desarrollar un marco normativo integral para la violencia digital. La llamada "Ley Olimpia", promulgada en 2021, introdujo reformas tanto en el Código Penal Federal como en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.

Su principal impulsora, Olimpia Coral Melo, promovió la visibilización de la difusión no consentida de material íntimo como una forma específica de violencia de género, esta vez, en el ámbito digital. El artículo 20 quáter de la Ley General de Acceso establece que la violencia digital comprende toda acción dolosa realizada mediante TICs que vulnere la integridad, dignidad o reputación de una persona, mientras que el artículo 199 octies del Código Penal Federal tipifica esta clase de conductas como una "violación a la intimidad sexual" .

La conocida como "Ley Ingrid" fue promulgada en 2023 y surgió a raíz del feminicidio de Ingrid Escamilla y la posterior difusión de imágenes de la víctima en redes sociales. Implicó la reforma del artículo 225 al Código Penal Federal, que contempla sanciones a servidores públicos o personas con acceso a información judicial que difundan imágenes, audios o videos de víctimas.

Las entidades federativas que componen la federación mexicana han adoptado reformas inspiradas en la Ley Olimpia, aunque con variaciones en las definiciones y penas en expectativa. Este proceso de armonización demuestra la progresiva incorporación del enfoque de género y derechos humanos al ámbito penal mexicano, aunque persisten desafíos en la aplicación práctica y en la capacitación judicial. Solo a modo de ejemplo pueden mencionarse las reformas promovidas en los códigos penales de los Estados de Nuevo León (última reforma de 2022), Ciudad de México (2020), Yucatán (2022).

3.3. Argentina y la Ley 27.736 (Ley Olimpia Argentina)

La Ley 27.736, sancionada en 2023, constituye la respuesta de dicho país a la violencia de género que se produce en espacios digitales. Inspirada en la experiencia mexicana, reformó la Ley 26.485 de Protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres de modo de incluir la "violencia digital o telemática" como modalidad específica. Esa normativa reconoce los derechos digitales, la reputación digital y la dignidad de las mujeres como bienes jurídicos protegidos y establece la obligación del Estado de garantizar su desenvolvimiento libre y seguro en entornos digitales. Además, amplía la definición de violencia de género a los contextos digitales y telemáticos.

3.4. Convergencia con estándares internacionales y desafíos futuros

Puede pensarse que la convergencia entre las leyes sancionadas a nivel local y los estándares internacionales en materia de violencia de género refleja un proceso de expansión del paradigma protectorio del derecho a una vida libre de violencia hacia espacios no contemplados hasta el presente, en concreto, los entornos digitales. Tanto la Ley Olimpia mexicana como la Ley 27.736 argentina materializan los compromisos asumidos por dichos países en la Convención CEDAW y la Convención de Belém do Pará.

En este sentido, el Comité CEDAW y la Corte Interamericana han instado a los Estados a implementar políticas públicas integrales, que combinen medidas penales con estrategias preventivas, educativas y tecnológicas. El principio de debida

diligencia reforzada implica que la omisión estatal frente a la violencia digital puede generar responsabilidad internacional. Por tanto, los Estados deben desarrollar mecanismos de monitoreo, cooperación transnacional y reparación integral que garanticen el pleno ejercicio de los derechos digitales de las mujeres. En los próximos acápites quedarán de resalto algunos de los desafíos a futuro en esta materia.

4. Tensiones aparentes entre la sanción de la violencia digital y la libertad de expresión

El abordaje jurídico de la violencia de género digital enfrenta uno de sus mayores desafíos en la aparente tensión entre el deber estatal de prevenir, sancionar y erradicar esas formas de violencia y la garantía del derecho a la libertad de expresión. La difusión no consentida de contenidos íntimos, el acoso digital o la reproducción de discursos de odio por motivos de género exigen una respuesta estatal eficaz, pero tal intervención no puede desconocer los límites impuestos por los estándares internacionales sobre libertad de expresión y censura previa. El reto consiste en encontrar un punto de equilibrio que asegure la protección efectiva de los derechos de las mujeres sin afectar indebidamente las garantías democráticas de libre difusión de ideas e información.

4.1. Modelos globales de regulación de Internet

A nivel internacional se identifican tres grandes modelos de regulación de la actividad en línea. El modelo liberal o privatista, representado por Estados Unidos, se basa en la autorregulación del mercado y la exención de responsabilidad de los proveedores de servicios (conforme la Sección 230 de la Ley de "Decencia en las Comunicaciones" o Communications Decency Act, 1996), lo que otorga a las plataformas amplias facultades para decidir qué contenidos alojar o remover. En contraposición, el modelo estatal o restrictivo, adoptado por países como China, establece un control gubernamental directo sobre los flujos de información, priorizando la seguridad nacional y el orden público. Finalmente, el modelo europeo o de regulación mixta, plasmado en la Directiva sobre Comercio Electrónico (2000/31/CE) y la Ley de Servicios Digitales (2022), ambos del Parlamento Europeo y el Consejo de la Unión Europea, que busca equilibrar derechos en conflicto mediante el establecimiento de responsabilidad condicionada de los intermediarios al principio del "conocimiento efectivo", es decir, al concreto anoticiamiento que se tenga del contenido ilícito del contenido cuestionado y la verificación de una falta de actuación diligente para removerlo o bloquearlo.

4.2. Responsabilidad de intermediarios. El caso argentino y la experiencia regional

En Argentina, la Corte Suprema de Justicia de la Nación en el caso "Belén Rodríguez c. Google Inc." (2014) estableció un criterio de responsabilidad subjetiva de los intermediarios. Afirmó que los buscadores no responden objetivamente por contenidos generados por terceros, salvo que exista conocimiento efectivo del material dañoso y omisión de medidas diligentes para su remoción. Este precedente, inspirado en la jurisprudencia europea (caso "Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (C-131/12, 2014)"), excluye la obligación de monitoreo previo y reafirma la protección constitucional de la libertad de expresión, que únicamente cederá ante la comprobación de un conocimiento de la

existencia de esa clase de contenido por parte del intermediario y la consecuente inacción de su parte frente al pedido de su retiro (art. 14 CN; art. 13 CADH).

Brasil, mediante su Marco civil de internet (Ley 12.965, 2014), consagra principios, garantías, derechos y obligaciones para el uso de internet en dicho país. Puntualmente, en el artículo 3, inciso VI, reconoce la responsabilidad de los agentes conforme a las actividades que ellos mismos desarrollen. En sintonía con el artículo 18 sobre responsabilidad de intermediarios, se fija como principio que los proveedores no podrán ser responsabilizados por daños resultantes de contenido generado por terceros. Asimismo, el criterio del "conocimiento efectivo" se desprende del artículo 19 que establece que los proveedores de aplicaciones de internet solo podrán ser responsables cuando, después de una orden judicial específica que identifique claramente el contenido ilícito, no tomen las medidas necesarias para retirarlo de la web. Este esquema se alinea con los Principios de Manila sobre responsabilidad de intermediarios de internet (2015) que exigen que toda restricción de contenidos cumpla los criterios de legalidad, necesidad y proporcionalidad, además de garantizar el debido proceso.

4.3. La experiencia mexicana: Ley Olimpia, Ley Ingrid y vacíos regulatorios

En México, tal como se mencionó, la Ley Olimpia modificó el Código Penal Federal y la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia para tipificar la violencia digital con motivos de género. Sin embargo, no establece obligaciones claras para las plataformas respecto de la remoción de contenido o la implementación de mecanismos de respuesta inmediata ante denuncias. La Ley Ingrid (2023) tampoco desarrolla un régimen de responsabilidad para intermediarios digitales. De este modo, puede afirmarse que el sistema mexicano, tanto a nivel federal como estadual, termina por priorizar la persecución individual de los autores materiales en cada caso llevado a conocimiento del sistema de justicia, sin avanzar hacia una regulación integral de las plataformas tecnológicas y la circulación en ellas de contenido gravoso.

4.4. Estándares internacionales de libertad de expresión y sus límites

El artículo 13 de la Convención Americana sobre Derechos Humanos reconoce la libertad de pensamiento y de expresión a través de la consagración del derecho a buscar, recibir y difundir información, prohibiendo la censura previa. Sin embargo, el inciso 2 autoriza ciertas restricciones que deben ser declaradas por ley y estipula que pueden aplicarse únicamente cuando sean necesarias para proteger los derechos o la reputación de otros, la seguridad nacional o el orden público. La Corte Interamericana en su jurisprudencia sostuvo que la libertad de expresión no es absoluta y debe armonizarse con otros derechos fundamentales mediante el test tripartito de legalidad, finalidad legítima y proporcionalidad ("Kimel vs. Argentina", 2008; "Palamara Iribarne vs. Chile", 2005).

Este estándar regional debe leerse en sintonía con los lineamientos del sistema internacional de protección de derechos, en particular, la Recomendación General 35 del Comité CEDAW que instó a los Estados a tipificar y sancionar la violencia digital, enfatizando la obligación de diligencia debida para prevenirla y garantizar la protección de las mujeres también en los entornos virtuales, y el Informe MESECVI-ONU Mujeres sobre Ciberviolencia y ciberacoso contra las mujeres y niñas (2022) que, en igual sentido, afirmó que las restricciones a la libertad de expresión resultan

legítimas cuando buscan evitar la difusión de discursos de odio o contenidos que perpetúan la violencia de género (pp. 76-79).

4.5. Armonización entre libertad de expresión y protección frente a la violencia digital

A partir de los estándares internacionales y las experiencias nacionales, puede afirmarse que el conflicto entre libertad de expresión y protección contra la violencia digital es solo aparente. No se trata de restringir el libre intercambio de ideas, sino de garantizar que el ejercicio de ese derecho no se convierta en un instrumento para reproducir violencias. El artículo 13 inciso 5 de la Convención Americana prohíbe expresamente toda apología del odio que constituya incitación a la violencia, lo que legitima la intervención estatal ante discursos misóginos o de incitación a la violencia sexual contra las mujeres.

En este sentido, los Estados deben adoptar medidas proporcionales y sujetas a control judicial que permitan bloquear o eliminar contenidos violentos, imponer obligaciones de diligencia a las plataformas y garantizar mecanismos efectivos de reparación. La protección de las mujeres frente a la violencia digital constituye una obligación derivada de los tratados internacionales de derechos humanos y de los principios de debida diligencia estatal. Los Estados deben armonizar la garantía de la libertad de expresión con el derecho de las mujeres a una vida libre de violencia, bajo el paradigma de una Internet libre, segura e inclusiva (Relatoría especial para la libertad de expresión, 2017).

5. Actuación de los Estados frente a un caso de violencia de género digital

La actuación de los Estados frente a los casos de violencia de género digital constituye una obligación derivada del principio de debida diligencia reforzada, conforme lo establece la Convención de Belém do Pará (art. 7 inciso b). Este principio impone a los Estados la obligación de actuar con celeridad, eficacia y sensibilidad de género en la prevención, investigación, sanción y reparación de esa clase de hechos.

En el contexto digital, dicha diligencia implica la adopción de medidas urgentes para preservar la evidencia electrónica y garantizar la seguridad de las víctimas. La investigación debe realizarse de manera inmediata, exhaustiva y dentro de plazos razonables, asegurando la preservación de datos informáticos relevantes. En este sentido, la intervención de cuerpos especializados en delitos informáticos resulta esencial para garantizar la integridad probatoria y el resguardo de la información (art. 9 de la Ley 27.736 Ley Olimpia Argentina).

Asimismo, las autoridades deben ordenar de inmediato el cese de los actos de perturbación, acoso o intimidación (art. 10 de la Ley 27.736 Ley Olimpia Argentina). Esa obligación encuentra respaldo en el Informe de la Relatoría Especial sobre la violencia contra la mujer (ONU, 2018, párr. 103), que autoriza la emisión de órdenes judiciales de supresión del contenido perjudicial y de medidas cautelares que impidan su redistribución, en colaboración con los intermediarios de Internet.

De igual modo, el artículo 12 de la Ley 27.736 argentina faculta a la autoridad judicial a ordenar la supresión, rectificación o actualización del contenido digital cuestionado. Para ello, el mandato debe identificar claramente la URL o el material específico cuya eliminación se ordena, resguardando así el debido proceso y la proporcionalidad de la medida.

Finalmente, pueden dictarse medidas complementarias como la prohibición de contacto o comunicación por medios digitales entre el agresor y la víctima (art. 11 de la Ley 27.736), en miras de prevenir revictimizaciones y garantizar el acceso efectivo a la justicia en un entorno seguro.

En suma, la actuación estatal frente a la violencia digital debe articular un enfoque integral basado en la debida diligencia reforzada frente a un caso particular y, de forma general, la adopción de políticas públicas que fortalezcan las capacidades institucionales para la prevención, investigación y reparación de las violencias de género en el entorno digital.

6. Derecho al olvido

El derecho al olvido se configura como una expresión contemporánea del derecho a la intimidad, la honra, la vida privada y la autodeterminación informativa. En términos generales, consiste en la facultad que asiste a toda persona a solicitar la eliminación, bloqueo o desindexación de información personal disponible en Internet que resulte obsoleta, irrelevante, inexacta o lesiva de sus derechos personalísimos. Tal como sostiene Zerda, implica la potestad "que tiene el/la titular de datos o informaciones personales, para solicitar que esa información o material o contenido dañoso sea eliminado, bloqueado, desindexado de los lugares donde aparece publicado, por encontrarse afectado ciertos derechos personalísimos, como su intimidad u honor" (2021: 196).

Este derecho encuentra sustento en el artículo 11 de la Convención Americana, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 12 de la Declaración Universal de Derechos Humanos, todos ellos protectores de la vida privada y la honra. Asimismo, se vincula con los denominados derechos ARCO —acceso, rectificación, cancelación y oposición— reconocidos en múltiples legislaciones nacionales, como mecanismos de control ciudadano sobre el uso de los datos personales.

El punto de inflexión en el reconocimiento del derecho al olvido se produce con la sentencia del Tribunal de Justicia de la Unión Europea en el ya mencionado caso "Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (C-131/12, 2014)", donde se reconoció el derecho de los ciudadanos a solicitar la desindexación de información personal en motores de búsqueda cuando resulte lesiva o carente de interés público actual. El tribunal estableció que los motores de búsqueda actúan como responsables del tratamiento de datos personales y, por tanto, deben atender solicitudes de eliminación justificadas. Este fallo es la antesala del Reglamento General de Protección de Datos del Parlamento Europeo y el Consejo de la Unión Europea (2016/679), que formalizó el derecho a la supresión o "derecho al olvido".

En el plano interamericano, si bien no existe aún una sentencia equivalente, los principios contenidos en los artículos 11 y 13 de la Convención Americana permiten armonizar la protección de la intimidad con la libertad de expresión bajo criterios de proporcionalidad y necesidad.

En Argentina, el derecho al olvido se encuentra tutelado a través del artículo 43 tercer párrafo, de la Constitución Nacional, que reconoce la acción de hábeas data, y de la Ley 25.326 de Protección de Datos Personales (2000), cuyo artículo 16 prevé el derecho de supresión o rectificación de datos inexactos o desactualizados. Como se refirió en párrafos anteriores, la jurisprudencia nacional consolidó su alcance en el precedente "Rodríguez, María Belén c. Google Inc." (2014), donde la

Corte Suprema de Justicia de la Nación sostuvo que los buscadores de Internet no son responsables de manera objetiva por los contenidos generados por terceros, pero deben actuar diligentemente cuando son notificados del carácter ilícito de la información.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) reconoce expresamente los derechos ARCO, que facultan a las personas a solicitar la cancelación o rectificación de datos personales cuando resulten incorrectos o afecten su intimidad (art. 22).

En América Latina, países como Brasil (Ley general de protección de datos, 2020) y Chile (Ley sobre protección de la vida privada, 2022) incorporan disposiciones similares.

Desde la mirada de los feminismos jurídicos, el derecho al olvido adquiere una dimensión reparadora frente a la violencia digital por motivos de género. En contextos donde la difusión no consentida de material íntimo refuerza las desigualdades existentes en materia de ejercicios de las sexualidades, la posibilidad de solicitar la desindexación o eliminación del contenido se erige como un acto de restitución de la autonomía y la dignidad de las mujeres. Autoras como Citron (2022) destacan que el derecho a la privacidad digital debe concebirse como una herramienta estratégica frente a esta clase de violencias.

El vínculo entre el derecho al olvido y la violencia de género digital es claro. La difusión no consentida de imágenes íntimas, el acoso o el hostigamiento en línea afectan derechos reconocidos en tratados internacionales, como la dignidad, la integridad y la honra. La posibilidad de solicitar la eliminación o desindexación del material difundido sin consentimiento constituye una forma de reparación integral y de prevención de la revictimización.

Tal como se refirió, el Informe del MESECVI-ONU Mujeres sobre Ciberviolencia y ciberacoso contra las mujeres y niñas (2022) insta a los Estados a garantizar mecanismos ágiles de eliminación de contenido digital violento y a imponer a los intermediarios tecnológicos obligaciones de respuesta diligente ante solicitudes de retiro de material.

En definitiva, el derecho al olvido constituye un instrumento indispensable para equilibrar el derecho a la libertad de expresión y el acceso a la información con la protección de la dignidad y la vida privada de las mujeres que acuden al sistema de justicia en busca de una respuesta frente a las violencias que sufren en el ámbito digital.

7. Conclusiones

El avance vertiginoso de las tecnologías de la información y la comunicación ha transformado la forma en que las personas interactúan, pero también ha generado nuevos espacios donde las violencias de género se reproducen y amplifican. Frente a este fenómeno, los Estados tienen la obligación de adoptar medidas integrales, conforme a los compromisos asumidos en instrumentos internacionales como la Convención CEDAW y la Convención de Belém do Pará. En virtud de esos instrumentos, los Estados deben actuar con debida diligencia reforzada para prevenir, sancionar y erradicar toda forma de violencia, incluida aquella que se manifiesta mediante las TICs.

El desafío jurídico contemporáneo radica en construir un marco normativo que no derive en actos de censuras, pero que tampoco perpetúe la desigualdad

estructural, orientando la regulación hacia la responsabilidad compartida entre el Estado, las plataformas tecnológicas y la sociedad civil.

7.1. Educación y alfabetización digital con perspectiva de género

Una política pública estratégica en materia de lucha contra estas violencias debe incluir proyectos de alfabetización y formación digital, entendida no sólo como el dominio técnico de herramientas digitales, sino como la formación crítica, ética y de género para habitar los entornos digitales con responsabilidad y seguridad, buscando fortalecer las capacidades ciudadanas para identificar, denunciar y prevenir la ciberviolencia. La alfabetización y educación en la cultura digital con enfoque de derechos humanos permite desnaturalizar prácticas sexistas y promover una convivencia en el espacio digital responsable e igualitaria.

A modo de ejemplo, el Ministerio de Educación de Ecuador puso en marcha la campaña "El mundo virtual de Eugenia", que tiene por objeto promover el uso adecuado de internet por parte de los niños, niñas y adolescentes. La campaña está dividida en tres bloques: el abordaje de los riesgos cibernéticos (contempla los tipos de delitos y las herramientas de protección), el uso saludable y responsable de las tecnologías y eventos de formación dirigidos a docentes y estudiantes (ONU Mujeres - MESECVI, 2022: 65).

Los programas educativos con perspectiva de género y enfoque interseccional son fundamentales para prevenir las violencias digitales y fomentar el respeto en los entornos virtuales. En este sentido, el ejemplo de Perú constituye un modelo regional atendible.

7.2. Cooperación internacional y ciberseguridad

Dado el carácter transnacional de la violencia digital, la cooperación internacional es indispensable. El Convenio de Budapest sobre Ciberdelincuencia (2001) constituye el principal marco internacional para la armonización legislativa y la cooperación judicial en materia de delitos informáticos[5]. Insta a los Estados a fortalecer sus capacidades institucionales en investigación digital, conservación de evidencia electrónica y asistencia judicial mutua (art. 23).

La apuesta por la cooperación multilateral de ningún modo puede excluir a las empresas tecnológicas y proveedores de servicios, quienes tienen la responsabilidad social de implementar mecanismos ágiles para prevenir la difusión de contenido violento o no consentido.

7.3. Responsabilidad de intermediarios y plataformas digitales

Los Principios de Manila (2015) sobre responsabilidad de intermediarios ofrecen un estándar internacional que equilibra el derecho a la libertad de expresión con la protección contra la violencia digital. Dichos principios establecen que los intermediarios no deben ser responsables por el contenido generado por terceros, salvo que exista orden judicial específica que disponga su retiro. Asimismo, las restricciones deben cumplir con los estándares de legalidad, necesidad y proporcionalidad, principios previstos en el artículo 13 de la Convención Americana

[5] Ratificado por Argentina en 2017. México aún no ha ratificado dicho convenio.

y en la jurisprudencia interamericana (los ya mencionados casos "Kimel vs. Argentina", 2008 y "Palamara Iribarne vs. Chile", 2005).

En ese sentido, los Estados deben establecer obligaciones de diligencia reforzada para las empresas tecnológicas cuando estas tomando conocimiento de la existencia de contenido dañoso en sus bases de datos.

7.4. Vías de reparación integral y acceso a la justicia

Más allá de la respuesta penal, las víctimas deben contar con vías de reparación integral que comprendan mecanismos civiles y administrativos. En Argentina, el Código Civil y Comercial reconoce la protección de la vida privada (art. 1770) y el derecho a la imagen (art. 53), mientras que la Ley 26.485, en su artículo 35, habilita acciones reparatorias frente a la violencia de género. Estos instrumentos permiten articular el derecho a la reparación civil con los estándares internacionales en la materia (Recomendación General 35 del Comité CEDAW) sobre la obligación estatal de investigar, sancionar y reparar las violaciones de derechos humanos.

El fortalecimiento de las capacidades judiciales es crucial. La formación en perspectiva de género e interseccionalidad debe ser transversal en el sistema de justicia, incorporando la comprensión de las nuevas tecnologías como medio de agresión y reproducción de desigualdades.

Para finalizar, la violencia digital de género constituye una extensión contemporánea de la desigualdad estructural. Su abordaje exige respuestas estatales articuladas que conjuguen la prevención, la sanción, la reparación y la educación transformadora. La actuación estatal debe inspirarse en el principio de debida diligencia reforzada y en los estándares internacionales de derechos humanos. Solo mediante políticas públicas sostenidas, cooperación internacional efectiva y regulación con perspectiva de género será posible garantizar una ciudadanía digital plena, inclusiva y libre de violencias.

Referencias bibliográficas

Citron, D. K. (2016). Hate Crimes in Cyberspace. Cambridge: Harvard University Press.

Citron, D. K. (2022). The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age. Nueva York: W.W. Norton & Company.

Citron, D., - Franks, M. A. (2014). Criminalizing Revenge Porn. Wake Forest Law Review, 49, 345–383.

Franks, M. A. (2019). The Cult of the Constitution: Our Deadly Devotion to Guns and Free Speech. California: Stanford University Press.

Sequeira, Leslie (2021). Sextorsion. Una nueva manifestación de violencia contra las mujeres basada en género. Suiza: The Global Initiative Against Transnational Organized Crime.

Zerda, M. (2021). Violencia de género digital. Buenos Aires: Editorial Hammurabi.

Mazzaferri, Laura y Roteta, Laura (2022). Sextorsión. Cuando se cruzan la corrupción y la violencia de género. En Colección Tópicos de la justicia penal federal. Tomo 1. Corrupción. Editores del Sur.

Legislación y jurisprudencia

Cámara de Diputados de la Nación Argentina (2022). Proyecto de Ley Belén, Expediente 2757-D-2022.

Comisión IDH (2017). Estándares para una Internet libre, abierta e inclusiva. Relatoría especial para la libertad de expresión.

Comité CEDAW (2017). Recomendación General 35 sobre la violencia por razón de género contra la mujer.

Comité DESC (2016). Observación General 22 relativa al derecho a la salud sexual y reproductiva.
Congreso de la Nación Argentina (2000). Ley 25.326 de Protección de datos personales.
Congreso de la Nación Argentina (2009). Ley 26.485 de Protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres.
Congreso de la Nación Argentina (2023). Ley 27.736, Ley Olimpia Argentina.
Congreso de los Estados Unidos de Norteamérica (1996). Communications Decency Act.
Congreso Nacional de Brasil (2014). Ley 12.965, Marco civil de internet.
Congreso Nacional de Brasil (2020). Ley 13.709, Ley general de protección de datos.
Congreso Nacional de Chile (2022). Ley 19.628 sobre protección de la vida privada (última modificación).
Consejo de Europa (2001). Convenio de Budapest sobre Ciberdelincuencia.
Corte IDH. Caso "Velásquez Rodríguez vs. Honduras", sentencia del 29 de julio de 1988, Fondo, Serie C 4.
Corte IDH. Palamara Iribarne vs. Chile, sentencia de 22 de noviembre de 2005, Fondo, Reparaciones y Costas, Serie C 135.
Corte IDH. Kimel vs. Argentina, sentencia de 2 de mayo de 2008, Fondo, Reparaciones y Costas, Serie C 177.
Corte IDH. Caso "González y otras (´Campo Algodonero´) vs. México", sentencia del 16 de noviembre de 2009, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C 205.
Corte IDH. Caso "Fernández Ortega vs. México", sentencia del 30 de agosto de 2010, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C 224.
Corte IDH. Caso "Atala Riffo y Niñas vs. Chile", sentencia del 24 de febrero de 2012, Fondo, Reparaciones y Costas, Serie C 239.
Corte Suprema de Justicia de la Nación Argentina. Rodríguez, María Belén c/ Google Inc. y otro s/ daños y perjuicios, sentencia del 28 de octubre de 2014, Fallos 337:1174.
Diario Oficial de la Federación, México (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Diario Oficial de la Federación, México (2021). Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, Ley Olimpia.
Diario Oficial de la Federación, México (2023). Decreto que reforma el artículo 225 del Código Penal Federal, Ley Ingrid.
OEA (1969). Convención Americana sobre Derechos Humanos.
OEA (1994). Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer.
ONU (1948). Declaración Universal de Derechos Humanos.
ONU (1966). Pacto Internacional de Derechos Civiles y Políticos.
ONU (1966). Pacto Internacional de Derechos Económicos, Sociales y Culturales.
ONU (1979). Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer.
ONU (2018). Informe de la Relatoría Especial sobre la violencia contra la mujer, sus causas y consecuencias (A/HRC/38/47).
ONU Mujeres (2021). Informe La violencia en línea contra las mujeres y las niñas.
ONU Mujeres - MESECVI (2022). Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará.
Parlamento del Reino Unido (2019). Ley para tipificar como delito determinados actos de voyeurismo y para fines conexos.
Parlamento Europeo y del Consejo (2016). Reglamento General 2016/679 de Protección de Datos.
Parlamento Europeo y del Consejo (2000). Directiva 2000/31/CE, relativa al comercio electrónico.
Parlamento Europeo y del Consejo (2022). Ley de Servicios Digitales 2022/2065, establece un mercado único de servicios digitales.
Principios de Manila sobre responsabilidad de intermediarios (2015).
Supremo Tribunal de Justicia de la Unión Europea (2014). Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, sentencia del 13 de mayo de 2014, C 131/12.